УТВЕРЖДЕНО
ПФНА.501410.001 РЭ-ЛУ

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ В ВИРТУАЛЬНЫХ ИНФРАСТРУКТУРАХ

Dallas Lock

(версия 4.68)

Руководство по эксплуатации

ПФНА.501410.001 РЭ

Листов 250

Аннотация

Данное руководство по эксплуатации освещает вопросы по установке, настройке и сопровождению системы защиты информации в виртуальных инфраструктурах Dallas Lock и предназначено для лиц, ответственных за ее эксплуатацию.

Руководство по эксплуатации подразумевает наличие у пользователя навыков работы в операционных системах Windows и Linux, с платформами VMware vSphere и oVirt/zVirt/HOSTVM/ РЕД Виртуализация, гипервизорами VMware ESXi, Hyper-V и KVM.

В документе представлены элементы графических интерфейсов, которые соответствуют эксплуатации Центра управления СЗИ ВИ в ОС Windows 7, 10 и Windows Server 2012 R2. Следует обратить внимание, что элементы графического интерфейса могут иметь незначительные отличия от представленных.

Содержание

Содержание **3**
ВВЕДЕНИЕ **6**
ТЕРМИНЫ И СОКРАЩЕНИЯ **7**
1 НАЗНАЧЕНИЕ И ВОЗМОЖНОСТИ СЗИ ВИ **12**
1.1 Возможности 12
2 РАЗВЕРТЫВАНИЕ И УДАЛЕНИЕ СЗИ ВИ **16**
2.1 Требования к аппаратному и программному обеспечению 16
2.2 Ограничения при установке и эксплуатации 19
2.2.1 Различие редакций СЗИ ВИ 21
2.3 Порядок развертывания компонентов 22
2.3.1 Порядок развертывания СЗИ ВИ для VMware vSphere vCenter 22
2.3.2 Порядок развертывания СЗИ ВИ для VMware vSphere vCSA 22
2.3.3 Порядок развертывания СЗИ ВИ для Hyper-V 22
2.3.4 Порядок развертывания СЗИ ВИ для KVM 23
2.3.5 Порядок развертывания СЗИ ВИ для oVirt/zVirt/HOSTVM/РЕД Вирт 23
2.4 Подготовка к установке СЗИ ВИ 23
2.4.1 Предварительная подготовка 23
2.4.2 Особенности установки 24
2.5 Развертывание СЗИ ВИ 25
2.5.1 Установка компонента «Центр управления СЗИ ВИ Dallas Lock» 25
2.5.2 Развертывание СЗИ ВИ для VMware vSphere vCenter 31
2.5.3 Развертывание СЗИ ВИ для VMware vSphere vCSA 38
2.5.4 Развертывание СЗИ ВИ для Hyper-V 40
2.5.5 Развертывание СЗИ ВИ для KVM 44
2.5.6 Развертывание СЗИ ВИ для oVirt/zVirt/HOSTVM/РЕД Вирт 45
2.6 Развертывание компонентов СЗИ ВИ с помощью мастера 47
2.6.1 Развертывание СЗИ ВИ для VMware vSphere vCenter 47
2.6.2 Развертывание СЗИ ВИ для VMware vSphere vCSA 52
2.6.3 Развертывание СЗИ ВИ для Hyper-V 53
2.6.4 Развертывание СЗИ ВИ для KVM 55
2.6.5 Развертывание СЗИ ВИ для oVirt/zVirt/HOSTVM/РЕД Вирт 55
2.7 Установка учетных данных 56
2.7.1 Установка учетных данных для vSphere 57
2.7.2 Установка учетных данных для гипервизора KVM 57
2.7.3 Установка учетных данных для СВ oVirt/zVirt/HOSTVM/РЕД Вирт 57
2.8 Вывод серверов виртуализации из домена безопасности 58
2.9 Удаление СЗИ ВИ 58
2.9.1 Удаление Центра управления СЗИ ВИ Dallas Lock 58
2.9.2 Удаление агентов DL Windows 59
2.9.3 Удаление агента DL ESXi 61
2.9.4 Удаление агента DL vCSA 62
2.9.5 Удаление агента DL KVM 62
2.9.6 Удаление агентов DL oVirt/zVirt/HOSTVM/РЕД Вирт 63
2.10 Обновление системы защиты 63
2.10.1 Стандартное обновление 63
2.10.2 Обновление windows-клиентов с помощью программы обновления 63
2.11 О программе 64
3 ОПИСАНИЕ СРЕДСТВ АДМИНИСТРИРОВАНИЯ **66**
3.1 Консоль 66
3.2 Информационная панель 68
3.2.1 Дерево «Агенты Windows» 68
3.2.2 Дерево «Агенты ВИ» 72
3.3 Основные параметры 78
3.3.1 Основные параметры работы агентов Windows 79
3.3.2 Основные параметры работы ядра СЗИ ВИ 80
3.3.3 Основные параметры группы СВ vSphere 80
3.3.4 Основные параметры группы СВ Hyper-V 81
3.3.5 Основные параметры группы KVM 81
3.4 Ролевая модель учетных записей СУД 82
3.4.1 Создание, изменение и удаление назначений ролей 83
3.5 Синхронизация 84
3.6 Сигнализация об НСД 84
3.7 Неактивный режим 87
3.7.1 Мягкий режим 88
3.8 Наследование настроек 89
3.9 Значок блокировки на панели задач 89
4 ОПИСАНИЕ СРЕДСТВ АУДИТА **90**

4.1 Веб-консоль ... 90
4.2 Информационная панель ... 91
4.2.1 Дерево «Агенты Windows» ... 91
4.2.2 Дерево «Агенты ВИ» ... 93
5 ПОДСИСТЕМА УПРАВЛЕНИЯ ПОЛЬЗОВАТЕЛЯМИ ... 95
5.1 Управление учетными записями ... 95
5.1.1 Полномочия на управление учетными записями ... 95
5.1.2 Управление учетными записями клиентов Windows ... 95
5.1.3 Управление учетными записями ВИ ... 103
5.1.4 Активация и деактивация учетных записей ... 109
5.1.5 Заблокированные пользователи ... 111
5.1.6 Удаление учетных записей ... 113
5.1.7 Смена пароля ... 113
5.2 Управление группами пользователей ... 114
5.2.1 Управление группами пользователей клиентов Windows ... 114
5.2.2 Управление группами пользователей ВИ ... 115
5.2.3 Удаление группы ... 121
5.3 Настройки параметров безопасности для объектов ВИ ... 121
5.3.1 Настройки параметров безопасности ... 121
5.4 Настройки параметров для клиентов Windows ... 127
5.4.1 Полномочия на управление параметрами безопасности ... 127
5.4.2 Разрешение и запрет интерактивного и удаленного входов в ОС ... 128
5.4.3 Настройка параметров безопасности ... 129
5.4.4 Настройка средств аппаратной идентификации ... 133
5.5 Аппаратная идентификация пользователя ... 139
5.5.1 Назначение аппаратной идентификации ... 139
5.5.2 Принудительная двухфакторная аутентификация ... 141
5.5.3 Снятие аппаратной идентификации ... 141
5.5.4 Дополнительные возможности аппаратной идентификации ... 141
5.5.5 Вход с использованием смарт-карт с сертификатом УЦ Windows ... 144
5.5.6 Вход с аппаратным идентификатором ... 145
5.6 Ключи удаленного доступа ... 146
6 ПОДСИСТЕМА УПРАВЛЕНИЯ ДОСТУПОМ ... 148
6.1 Разграничение доступа к объектам ФС ОС Windows ... 148
6.1.1 Дескрипторы объектов ... 148
6.1.2 Дискреционный доступ ... 149
6.1.3 Дескрипторы по пути ... 158
6.2 Контроль устройств в ОС Windows ... 159
6.2.1 Разграничение доступа к устройствам ... 160
6.2.2 Аудит доступа к устройствам ... 161
6.3 Удаленный доступ к СВ ... 162
6.3.1 Правила управления СВ ... 162
6.3.2 Клиенты управления СВ ... 162
6.4 Ролевая модель учетных записей СВ ... 164
6.4.1 Ролевая модель учетных записей vSphere ... 164
6.4.2 Ролевая модель учетных записей Hyper-V ... 167
6.4.3 Ролевая модель учетных записей KVM ... 169
6.4.4 Ролевая модель учетных записей oVirt/zVirt/HOSTVM/РЕД Вирт ... 170
6.4.5 Права пользователей ... 172
6.5 Настройка фильтрации трафика гипервизоров ESXi ... 181
6.6 Сегменты безопасности ... 183
6.6.1 Настройка сегментов безопасности ... 183
6.6.2 Сегмент безопасности с изолированной ВМ ... 187
6.7 Управление сессиями консолей ВМ ... 189
7 ПОДСИСТЕМА КОНТРОЛЯ ЦЕЛОСТНОСТИ ... 190
7.1 Контроль целостности файлов ... 190
7.1.1 Настройка контроля целостности СВ vSphere ... 191
7.1.2 Настройка контроля целостности СВ vCSA ... 191
7.1.3 Настройка контроля целостности гипервизора ESXi ... 191
7.1.4 Настройка контроля целостности СВ Hyper-V ... 192
7.1.5 Настройка контроля целостности гипервизора KVM ... 192
7.1.6 Настройка контроля целостности СВ oVirt/zVirt/HOSTVM/РЕД Вирт ... 193
7.1.7 Настройка контроля целостности гипервизора oVirt/zVirt/HOSTVM/РЕД Вирт ... 193
7.2 Настройка контроля целостности ВМ ... 194
7.2.1 Настройка контроля целостности конфигурации ВМ ... 194
7.2.2 Настройка контроля целостности для образов дисков ВМ ... 195
7.2.3 Настройка контроля целостности настроек безопасности ВМ ... 195
7.2.4 Проверка целостности конфигураций, дисков ВМ и настроек безопасности ВМ 196
7.3 Настройка параметров контроля целостности для клиентов Windows ... 196
7.3.1 Настройка политик контроля целостности ... 196

7.3.2 Настройка контроля целостности программно-аппаратной среды 197
7.3.3 Настройка политик контроля целостности для группы 197
7.3.4 Настройка параметров контроля целостности программно-аппаратной среды для группы 198
8 ПОДСИСТЕМА ГАРАНТИРОВАННОЙ ОЧИСТКИ ПАМЯТИ 200
8.1 Очистка остаточной информации из консоли на клиентах Windows 200
8.1.1 Удаление файлов и зачистка остаточной информации по команде 200
8.2 Очистка остаточной информации на объектах ВИ 202
8.2.1 Очистка остаточной информации из консоли на клиентах vSphere 202
8.2.2 Очистка остаточной информации из консоли на гипервизорах KVM/oVirt/zVirt/HOSTVM/РЕД Вирт 203
8.2.3 Удаление и зачистка виртуальной машины 203
8.2.4 Очистка информации с помощью утилиты Eraser 204
9 ПОДСИСТЕМА АУДИТА 206
9.1 Аудит гипервизоров 206
9.1.1 Аудит гипервизоров ESXi 206
9.1.2 Аудит гипервизоров Hyper-V 207
9.1.3 Журналы событий 208
9.1.4 Журнал ЦУ СЗИ ВИ 209
9.1.5 Журнал событий ВИ 210
9.1.6 Журнал сервера виртуализации 211
9.1.7 Журнал гипервизора (ESXi) 212
9.1.8 Журнал событий oVirt/zVirt/HOSTVM/РЕД Вирт 212
9.1.9 Системный журнал (KVM/oVirt/zVirt/HOSTVM/РЕД Вирт) 212
9.2 Аудит компьютеров клиентов Windows 213
9.2.1 Аудит событий на компьютерах клиентов Windows 213
9.2.2 Журналы событий на компьютерах клиентов Windows 216
9.2.3 Журнал Сервера УД 216
9.2.4 Формирование журналов событий на компьютерах клиентов Windows 217
9.2.5 Просмотр журналов событий на компьютерах клиентов Windows 218
10 ЕДИНЫЙ ЦЕНТР УПРАВЛЕНИЯ DALLAS LOCK 220
10.1 Ввод СЗИ ВИ в ДБ ЕЦУ 220
10.2 Вывод СЗИ ВИ из ДБ ЕЦУ 222
11 ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ 223
11.1 Сохранение конфигурации ЦУ СЗИ ВИ 223
11.2 Работа с логами 223
11.2.1 Включение логов виртуализации на ЦУ СЗИ ВИ и агентах Windows (Hyper-V, vCenter for Windows) 223
11.2.2 Включение логов НСД на ЦУ СЗИ ВИ и агентах Windows (Hyper-V, vCenter for Windows) 224
11.2.3 Включение логов на агентах Linux (ESXi, vCSA, KVM/oVirt/zVirt/HOSTVM/РЕД Вирт) 224
11.3 Настройки лицензирования 224
11.4 Шаблоны безопасности 225
11.5 Снапшоты 226
11.5.1 Ручное создание снапшота 226
11.5.2 Автоматическое снятие снапшотов 227
11.6 Создание отчета о параметрах безопасности и назначенных правах 228
11.7 Блокирование запуска ВМ 228
12 АВАРИЙНОЕ ОТКЛЮЧЕНИЕ СЗИ ВИ В РУЧНОМ РЕЖИМЕ 230
13 Приложение № 1 233
14 Приложение № 2 250
14.1 Добавление корневого сертификата СЗИ ВИ в доверенные корневые сертификаты VMware PSC 250

ВВЕДЕНИЕ

Данное руководство предназначено для администратора программного продукта «Система защиты информации в виртуальных инфраструктурах «Dallas Lock».

В руководстве содержатся сведения, необходимые для получения общего представления о системе защиты, ее функциональных возможностях, а также для установки, настройки и управления работой в соответствии с требованиями безопасности.

В данном руководстве описание работы с системой носит процедурный характер, то есть основное внимание сосредоточено на порядке выполнения тех или иных действий.

На сайте продукта (www.dallaslock.ru) можно получить дополнительную информацию о системе защиты в виртуальных инфраструктурах Dallas Lock, в предыдущих версиях, а также заказать комплекс услуг по проектированию, внедрению и сопровождению продукта.

Обращения в службу технической поддержки системы защиты в виртуальных инфраструктурах Dallas Lock осуществляются по электронному адресу: helpdesk@confident.ru.

Сайт компании-разработчика системы защиты в виртуальных инфраструктурах Dallas Lock ООО «Конфидент» доступен по ссылке: www.confident.ru.

ТЕРМИНЫ И СОКРАЩЕНИЯ

Термины *компьютер, ПК, рабочая станция, ТС* считаются эквивалентными и используются в тексте руководства.

Принятые сокращения

Сокращение	Полная формулировка
АУД	агент управления доступом
ВИ	виртуальная инфраструктура
ВМ	виртуальная машина
ДБ	домен безопасности
ЕЦУ	Единый Центр Управления Dallas Lock (ЕЦУ Dallas Lock)
Консоль	консоль Центра управления СЗИ ВИ Dallas Lock
КЦ	контроль целостности
ЛВС	локальная вычислительная сеть
МЭ	межсетевой экран
ОС	операционная система
ПЗУ	постоянное запоминающее устройство, энергонезависимая память, используемая для хранения массива неизменяемых данных
ПК	персональный компьютер
СВ	сервер виртуализации
Сервер УД	сервер управления доступом
СЗИ ВИ	система защиты информации в виртуальных инфраструктурах
СЛ	сервер лицензий
ТС	техническое средство
УЦ	удостоверяющий центр
ФС	файловая система
ЦУ СЗИ ВИ	Центр управления СЗИ ВИ
AD	Active Directory
SP (Service Pack)	пакет обновлений для операционной системы

Общая терминология

Сокращение	Полная формулировка
Виртуальная инфраструктура	информационная система, состоящая из целевых элементов (виртуальных машин, виртуальных коммутаторов и т.д.) и обеспечивающих их работу вспомогательных элементов (гипервизоров, серверов виртуализации, устанавливаемых на них ОС), позволяющая более эффективно управлять аппаратными ресурсами по сравнению с обычной ИТ-инфраструктурой (физическими серверами, рабочими станциями, коммутаторами и т.д.)
Гипервизор	программа или аппаратная схема, обеспечивающая или позволяющая одновременное, параллельное выполнение нескольких ОС на одном ТС
Объекты ВИ	элементы ВИ, такие как: СВ vCenter, СВ vCSA, СВ oVirt/zVirt/HOSTVM/РЕД Вирт, гипервизор oVirt/zVirt/HOSTVM/РЕД Вирт, гипервизор ESXi, гипервизор Hyper-V, гипервизор KVM, виртуальная машина, введенные под контроль данного Центра управления СЗИ ВИ и образующие домен безопасности
Платформа виртуализации	программное решение для создания виртуальной инфраструктуры (VMware vSphere, Microsoft Hyper-V, KVM, oVirt, zVirt, HOSTVM, РЕД Вирт),

Сокращение	Полная формулировка
	предоставляющее набор целевых и вспомогательных элементов для ее построения
Сервер виртуализации	вспомогательный компонент ВИ, сервер или ВМ с установленным на нем средством управления системой виртуализации
Контроль целостности	проверка соответствия контролируемого объекта эталонному образцу с использованием контрольных сумм
Контрольная сумма	некоторое значение, рассчитанное по набору данных путём применения определённого алгоритма и используемое для проверки целостности данных при их передаче или хранении
Снапшот	моментальный снимок, копия файлов и каталогов файловой системы на определённый момент времени

Терминология СЗИ ВИ Dallas Lock

Сокращение	Полная формулировка
Агент DL ESXi	компонент защиты гипервизора ESXi
Агент DL Hyper-V	компонент защиты гипервизора Hyper-V
Агент DL KVM	компонент защиты гипервизора KVM
Агент DL Engine	компонент защиты сервера виртуализации oVirt, zVirt, HOSTVM и РЕД Виртуализации
Агент DL Host	компонент защиты гипервизора oVirt, zVirt, HOSTVM и РЕД Виртуализации
Агент DL vCenter for Windows	компонент защиты сервера виртуализации vCenter
Агент DL vCSA	компонент защиты сервера виртуализации vCSA
Агент управления доступом	компонент СЗИ ВИ Dallas Lock, устанавливаемый на объекты ВИ (сервер vCenter for Windows, гипервизор Hyper-V, SC VMM, кластера Hyper-V) для обеспечения выполнения политик безопасности
Веб-сервер СЗИ ВИ	компонент Центра управления СЗИ ВИ Dallas Lock, обеспечивающий доступ к веб-интерфейсу и возможностям аудита СЗИ ВИ. Реализован в виде службы
Домен безопасности	организация политик безопасности совокупностью Центра управления СЗИ ВИ и агентов управления доступом на множестве объектов ВИ
Консоль Центра управления СЗИ ВИ	компонент Центра управления СЗИ ВИ Dallas Lock, средство администрирования СЗИ ВИ
Параметры безопасности (политики безопасности)	совокупность правил по обеспечению безопасности информации, выраженные настраиваемыми категориями системы защиты
Сервер управления доступом (Сервер УД)	компонент Центра управления СЗИ ВИ Dallas Lock, обеспечивающий защиту серверов виртуализации посредством взаимодействия с АУД. Входит в состав Ядра СЗИ ВИ
СЗИ ВИ Dallas Lock	программный комплекс, состоящий из Центра управления СЗИ ВИ и работающих под его управлением АУД, устанавливаемых в виртуальные инфраструктуры с целью обеспечения безопасности путем включения в ДБ их элементов

Сокращение	Полная формулировка
Центр управления СЗИ ВИ	совокупность программных компонентов АУД, сервера УД и ядра СЗИ ВИ, управляемая с помощью Консоли
Ядро СЗИ ВИ	компонент Центра управления СЗИ ВИ Dallas Lock, обеспечивающий централизованное управление объектами виртуальной инфраструктуры. Реализовано в виде службы

Терминология VMware

Сокращение	Полная формулировка
ESXi	гипервизор ESXi, средство виртуализации VMware vSphere
VMware vSphere	платформа виртуализации компании VMware
vCenter	VMware vCenter Server, сервер централизованного управления средством виртуализации ESXi, состоит из консоли управления vClient и сервиса vCenter, выполняющихся на ОС Windows, установленной на рабочую станцию
vCSA	VMware vCenter Server Appliance, сервер централизованного управления средством виртуализации ESXi, состоит из службы vCenter выполняющейся на ОС Photon, установленной в виртуальную машину внутри ВИ, доступ к службе vCenter осуществляется через веб-браузер с поддержкой Flash/HTML5
Linked Mode	механизм, который объединяет серверы vCenter и позволяет использовать единое пространство объектов в географически распределенных датацентрах
Enhanced Linked Mode (ELM)	технология, позволяющая объединить серверы vCSA и vCenter, используя один или несколько внешних серверов PSC для репликации ролей, разрешений, лицензий, политик
Embedded Linked Mode	технология, позволяющая объединить серверы vCSA со встроенным PSC в общий домен для синхронизации, репликации и резервного копирования данных
Hybrid Linked Mode (HLM)	технология, с помощью которой осуществляется работа облачного сервиса VMware Cloud on AWC (VMC) с локальным доменом vCenter Single Sign-On
Platform Services Controller (PSC)	сервис vSphere, выполняющий функции безопасности инфраструктуры, такие как лицензирование и управление сертификатами
VMware Fault Tolerance	технология, предназначенная для защиты виртуальных машин с помощью кластеров непрерывной доступности

Терминология Hyper-V

Сокращение	Полная формулировка
Hyper-V	гипервизор Hyper-V, средство виртуализации Microsoft Hyper-V
Microsoft Hyper-V	платформа виртуализации серверов/рабочих станций x64 компании Microsoft
Virtual Machine Manager	сервис управления виртуальными машинами

Терминология KVM

Сокращение	Полная формулировка
KVM	Kernel-based Virtual Machine, программное решение, обеспечивающее виртуализацию в среде Linux на платформе x86, которая поддерживает

Сокращение	Полная формулировка
	виртуализацию на базе Intel VT (Virtualization Technology) либо AMD SVM (Secure Virtual Machine)
QEMU	Quick Emulator, программа с открытым исходным кодом для эмуляции аппаратного обеспечения различных платформ

Терминология oVirt

Сокращение	Полная формулировка
oVirt	свободная, кроссплатформенная система управления виртуализацией, базирующаяся на технологии KVM
oVirt Engine	средство мониторинга и управления вычислительными узлами, хранилищами, сетями и виртуальными машинами. Далее по тексту сервер виртуализации oVirt (СВ oVirt)
oVirt Node	минимальная операционная система, основанная на CentOS, которая предназначена для работы в качестве гипервизора в среде oVirt
oVirt Host	вычислительный узел (гипервизор), на котором выполняются ВМ, а также могут быть размещены локальные хранилища. Далее по тексту гипервизор oVirt

Терминология zVirt

Сокращение	Полная формулировка
zVirt	система безопасного управления средой виртуализации. Построена на open source продуктах, создана на базе высокопроизводительного гипервизора KVM (Kernel-based Virtual Machine) и системы управления zVirt
zVirt Engine	средство мониторинга и управления вычислительными узлами, хранилищами, сетями и виртуальными машинами. Далее по тексту сервер виртуализации zVirt (СВ zVirt)
zVirt Node	минимальная операционная система, основанная на CentOS, которая предназначена для работы в качестве гипервизора в среде zVirt
zVirt Host	вычислительный узел (гипервизор), на котором выполняются ВМ, а также могут быть размещены локальные хранилища. Далее по тексту гипервизор zVirt

Терминология HOSTVM

Сокращение	Полная формулировка
HOSTVM	платформа виртуализации корпоративного уровня на основе гипервизора KVM для виртуализации серверов, рабочих столов и приложений
HOSTVM Manager	средство мониторинга и управления вычислительными узлами, хранилищами, сетями и виртуальными машинами. Далее по тексту сервер виртуализации HOSTVM (СВ HOSTVM)
HOSTVM	вычислительный узел (гипервизор), на котором выполняются ВМ, а также могут быть размещены локальные хранилища. Далее по тексту гипервизор HOSTVM

Терминология РЕД Виртуализация

Сокращение	Полная формулировка
РЕД Виртуализация	Система управления виртуализацией серверов и рабочих станций. Базируется на гипервизоре KVM (kernel-based virtual machine) и открытой платформе управления виртуальной инфраструктурой

Сокращение	Полная формулировка
РЕД Виртуализация Engine	средство мониторинга и управления вычислительными узлами, хранилищами, сетями и виртуальными машинами. Далее по тексту сервер виртуализации РЕД Вирт (СВ РЕД Вирт)
РЕД Виртуализация Node	минимальная операционная система, основанная на РЕД ОС, которая предназначена для работы в качестве гипервизора в среде РЕД Виртуализация
РЕД Виртуализация Host	вычислительный узел (гипервизор), на котором выполняются ВМ, а также могут быть размещены локальные хранилища. Далее по тексту гипервизор РЕД Вирт

1 НАЗНАЧЕНИЕ И ВОЗМОЖНОСТИ СЗИ ВИ

СЗИ ВИ Dallas Lock – система защиты информации в виртуальных инфраструктурах, которая предназначена для защиты среды виртуализации на базе технологий VMware vSphere (vCenter for Windows 5.5, 6.0, 6.5, 6.7 и vCSA 6.5, 6.7, 7.0 совместно с ESXi[1] аналогичной версии), Windows Server (Hyper-V) (версий 2012, 2012 R2, 2016, 2019, 2022), oVirt 4.4, zVirt (версий 3.0, 3.1), HOSTVM, РЕД Виртуализация 7.3 и KVM (использующей библиотеки libvirt (версии не ниже 4.5.0) в качестве инструмента управления гипервизором) от несанкционированного доступа при работе в многопользовательских автоматизированных системах, государственных информационных системах, в автоматизированных системах управления, информационных системах персональных данных и на объектах критической информационной инфраструктуры.

СЗИ ВИ Dallas Lock имеет две редакции: «Стандартная» и «Расширенная». Редакция СЗИ ВИ Dallas Lock «Расширенная» имеет ряд преимуществ перед редакцией «Стандартная» (подробнее см. п. 2.2.1 «Различие редакций СЗИ ВИ»).

1.1 Возможности

СЗИ ВИ Dallas Lock предоставляет следующие возможности:

1. Идентификация и аутентификация администраторов и пользователей в виртуальной среде по идентификатору и паролю условно-постоянного действия – на ЦУ СЗИ ВИ, серверах виртуализации vCenter, vCSA, oVirt, zVirt, HOSTVM, РЕД Вирт и гипервизорах Hyper-V, KVM, oVirt, zVirt, HOSTVM и РЕД Вирт. Контроль пользователей, имеющих право на вход на гипервизор, осуществляется посредством выполнения необходимых настроек на стороне ЦУ СЗИ ВИ и процесса синхронизации гипервизора с ЦУ СЗИ ВИ.
2. Контроль и аудит входа в среду VMware vSphere через механизм SSO.
3. Использовать в качестве средства опознавания пользователей ОС Windows следующие электронные идентификаторы:
   - USB-Flash накопители;
   - электронные ключи Touch Memory (iButton);
   - HID Proximity-карты;
   - USB-ключи Aladdin eToken Pro/Java;
   - смарт-карты Aladdin eToken Pro/SC;
   - USB-ключи и смарт-карты Рутокен (Rutoken) и Рутокен ЭЦП;
   - USB-ключи и смарт-карты JaCarta;
   - USB-ключи и смарт-карты ESMART;
   - NFC-метки и смарт-карты семейства MIFARE.
4. Запрет доступа к защищаемым ресурсам не идентифицированных пользователей и пользователей, подлинность идентификации которых при аутентификации не подтвердилась. Контроль пользователей, имеющих право на доступ к гипервизору, при условии успешной авторизации должен осуществляться посредством выполнения необходимых настроек на стороне ЦУ СЗИ ВИ и процесса синхронизации гипервизора с ЦУ СЗИ ВИ.
5. Управление средствами аутентификации, в том числе хранение, выдача и инициализация всех компонент защищаемой виртуальной инфраструктуры. Также осуществляется блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации для ЦУ СЗИ ВИ, СВ vCenter, СВ oVirt, СВ zVirt, СВ HOSTVM, СВ РЕД Вирт и гипервизоров Hyper-V, KVM, oVirt, zVirt, HOSTVM и РЕД Вирт.
6. Для решения проблемы «простых паролей» система имеет гибкие настройки сложности паролей. Можно задать минимальную длину пароля, необходимость обязательного наличия в пароле цифр, специальных символов, строчных и прописных букв, степень отличия нового пароля от старого и срок действия.
7. В СЗИ ВИ реализована система контроля целостности параметров ТС.

Для агентов DL vCSA, DL KVM, DL Engine и Host обеспечивается:

- контроль целостности файлов в директориях, указанных в переменной PATH;
- контроль целостности файлов в директориях «/lib» (включая все поддиректории) и «/usr/lib» (без поддиректорий);
- файлы агентов DL vCSA, DL KVM, DL Engine и DL Host.

Для агента DL ESXi обеспечивается:

[1] Для защиты среды виртуализации на базе гипервизора ESXi 5.5 необходимо применять сертифицированную версию изделия СЗИ ВИ Dallas Lock 376.3. С назначением, возможностями и требованиями к данной версии можно ознакомиться в документе «Руководство по эксплуатации» ИК1.

- контроль целостности файлов в директориях, указанных в переменной PATH;
- контроль целостности файлов в директориях (включая все поддиректории):
  - «/lib»;
  - «/usr/libexec/vmwauth»;
  - «/usr/lib/openwsman/authenticators»;
  - «/usr/lib/vmware/auth/bin»;
  - «/usr/lib/vmware/openssh/bin»;
  - «/usr/lib/vmware/rhttpproxy/bin»;
  - «/usr/lib/vmware/vmsyslog/bin»;
  - «/usr/lib/vmware/vsan/bin».
- контроль целостности файлов в директории «/usr/lib» (без поддиректорий);
- файлы агента DL ESXi.

Для агента DL Hyper-V и агента DL vCenter for Windows:

- контроль целостности системных файлов ВИ;
- контроль целостности образов дисков ВМ;
- контроль целостности конфигурационных файлов ВМ;
- контроль целостности настроек безопасности ВМ;
- контроль целостности аппаратной части гипервизоров.

Для контроля целостности используются контрольные суммы, вычисленные по одному из алгоритмов на выбор: CRC32, MD5.

Кроме того, СЗИ ВИ выполняет периодический контроль целостности ВМ.

8. СЗИ ВИ позволяет производить настройку правил фильтрации сетевого трафика гипервизора ESXi.

9. СЗИ ВИ в рамках поддержки требований безопасности для финансовых организаций в соответствии с ГОСТ Р 57580.1-2017 обеспечивает выполнение следующих требований[2]:

- Создание сегмента безопасности в полуавтоматическом режиме с доступом только для одного пользователя к выбранной ВМ.
- Контроль сессий пользователей ВМ при работе с консолей осуществляется централизовано из Консоли ЦУ СЗИ ВИ.
- Разделение виртуальной инфраструктуры vSphere и Hyper-V на сегменты безопасности, состоящие из ВМ и учетных записей/групп учетных записей, ограничивая сетевое взаимодействие между сегментами посредством технологии VLAN.
- Проверка целостности настроек параметров безопасности ВМ при ее запуске.

10. Реализовано разграничение доступа к компонентам виртуальной инфраструктуры – к ЦУ СЗИ ВИ, СВ vCenter, СВ oVirt, СВ zVirt, СВ HOSTVM, СВ РЕД Вирт и гипервизорам Hyper-V, KVM, oVirt, zVirt, HOSTVM и РЕД Вирт. Разграничение доступа к гипервизорам ESXi и файлам виртуальных машин реализуется в пределах ролевой модели разграничения доступа VMware vSphere 6.0/6.5/6.7/7.0. Разграничение доступа к гипервизорам Hyper-V и файлам виртуальных машин реализуется в пределах ролевой модели разграничения доступа Hyper-V. Разграничение доступа к гипервизорам KVM и файлам виртуальных машин реализуется в пределах ролевой модели разграничения доступа KVM. Разграничение доступа к СВ oVirt, zVirt, HOSTVM, РЕД Вирт и гипервизорам oVirt, zVirt, HOSTVM, РЕД Вирт и файлам виртуальных машин реализуется в пределах ролевой модели разграничения доступа oVirt, zVirt, HOSTVM, РЕД Вирт соответственно.

11. Контроль доступа к операциям, выполняемым с помощью средств управления виртуальными машинами, в том числе к операциям создания, запуска, остановки, создания копий, удаления виртуальных машин, которые должны быть разрешены только назначенным пользователям.

12. Разграничение доступа по дискреционному принципу к объектам файловой системы и устройствам в виртуальной среде – на ЦУ СЗИ ВИ, СВ vCenter и гипервизорах Hyper-V. Разграничение доступа к гипервизорам ESXi и файлам виртуальных машин реализуется в пределах ролевой модели разграничения доступа vSphere 6.0/6.5/6.7/7.0. Разграничение доступа к гипервизорам KVM и файлам виртуальных машин реализуется в пределах ролевой модели разграничения доступа KVM. Разграничение доступа к СВ oVirt, zVirt, HOSTVM, РЕД Вирт и гипервизорам oVirt, zVirt, HOSTVM, РЕД Вирт и файлам виртуальных машин реализуется в пределах ролевой модели разграничения доступа oVirt, zVirt, HOSTVM, РЕД Вирт соответственно.

13. При первоначальном назначении или при перераспределении внешней памяти СЗИ ВИ Dallas Lock предотвращает доступ субъекту к остаточной информации. Осуществляется

[2] Данные требования реализованы для среды виртуализации vSphere и Hyper-V.

очистка освобождаемых областей оперативной памяти ТС, освобождаемых областей памяти внешних накопителей. Очистка осуществляется однократной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов). На гипервизорах ESXi, oVirt, zVirt, HOSTVM и РЕД Вирт осуществляется очистка остаточной информации по отношению к дискам виртуальных машин.

14. Доступно создание снапшотов как в ручном режиме, так и в автоматическом (по расписанию и/или с заданным интервалом) для платформ виртуализации vSphere и Hyper-V.

15. В СЗИ ВИ реализовано ведение следующих журналов:

- Журнал ЦУ СЗИ ВИ. В журнал заносятся события, связанные непосредственно с работой ЦУ СЗИ ВИ.
- Журнал событий ВИ vSphere. Журнал событий ВИ содержит информацию об операциях над контролируемыми объектами на СВ, поступающую от агентов DL vCenter for Windows, DL vCSA.
- Журнал событий ВИ Hyper-V. Журнал событий ВИ содержит информацию об операциях над контролируемыми объектами на СВ, поступающую от агента DL Hyper-V.
- Журнал событий ВИ KVM/oVirt/zVirt/HOSTVM/РЕД Вирт. Журнал событий ВИ содержит информацию об операциях над контролируемыми объектами на СВ, поступающую от агента DL KVM и DL Engine.
- Журнал сервера виртуализации vCenter. Журнал содержит информацию об изменениях состояния управляемых объектов на СВ vCenter. События включают в себя действия системы и пользователей, которые происходят на объектах ВИ.
- Журнал сервера виртуализации Hyper-V. Журнал содержит информацию об изменениях состояния управляемых объектов на СВ Hyper-V. События включают в себя действия системы и пользователей, которые происходят на объектах ВИ.
- Журнал сервера виртуализации KVM. Журнал содержит информацию об изменениях состояния управляемых объектов на СВ KVM. События включают в себя действия системы и пользователей, которые происходят на объектах ВИ.
- Системный журнал сервера виртуализации KVM. Журнал содержит информацию о работе операционной системы.
- Журнал сервера виртуализации oVirt/zVirt/HOSTVM/РЕД Вирт. Журнал содержит информацию об изменениях состояния управляемых объектов на СВ oVirt/zVirt/HOSTVM/РЕД Вирт. События включают в себя действия системы и пользователей, которые происходят на объектах ВИ.
- Системный журнал сервера виртуализации oVirt/zVirt/HOSTVM/РЕД Вирт. Журнал содержит информацию о работе операционной системы.
- Системный журнал гипервизора oVirt/zVirt/HOSTVM/РЕД Вирт. Журнал содержит информацию о работе операционной системы.
- Журнал гипервизора ESXi. В журнале регистрируются события безопасности гипервизора ESXi, на котором установлен агент DL. Журнал включает в себя системные события и действия агента DL на гипервизоре ESXi.
- Журнал Сервера УД. Данный журнал содержит информацию о событиях, происходящих на подключенных клиентах.
- Журналы, которые ведутся отдельно на каждом АУД ОС Windows: журнал входов, журнал управления учетными записями, журнал ресурсов, журнал управления политиками, журнал процессов, журнал пакетов МЭ.

16. Для облегчения работы с журналами есть возможность фильтрации записей по определенному признаку и экспортирования журналов в различные форматы. При переполнении журнала, а также по команде администратора, его содержимое архивируется и помещается в специальную папку, доступ к которой есть, в том числе и через средства удаленного администрирования. Этим обеспечивается непрерывность ведения журналов.

17. Возможно использование предустановленных шаблонов типовых политик безопасности на основе требований следующих документов:

- Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации (утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.) (АС).
- ГОСТ Р 56938-2016. Защита информации. Защита информации при использовании технологий виртуализации. Общие положения.
- Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (ИСПДн).

- Методический документ. Меры защиты информации в государственных информационных системах (утвержден ФСТЭК России 11 февраля 2014 г.) (ГИС).
- Стандарт безопасности данных индустрии платежных карт (PCI DSS).
- Стандарт Банка России по обеспечению информационной безопасности организаций банковской системы Российской Федерации (СТО БР ИББС).

2 РАЗВЕРТЫВАНИЕ И УДАЛЕНИЕ СЗИ ВИ

Развертывание СЗИ ВИ Dallas Lock заключается в установке Центра управления СЗИ ВИ Dallas Lock на рабочую станцию, агентов управления доступом – в виртуальные инфраструктуры и включении их в домен безопасности.

Центр управления СЗИ ВИ состоит из Консоли управления СЗИ ВИ, сервера управления доступом и ядра СЗИ ВИ, устанавливаемых на рабочую станцию под управлением операционной системы семейства Windows (подробные характеристики ОС и аппаратной платформы см. в п. 2.1 «Требования к аппаратному и программному обеспечению»). Консоль является основным средством администрирования изделия (подробное описание см. в разделе 3 «ОПИСАНИЕ СРЕДСТВ АДМИНИСТРИРОВАНИЯ»).

Агенты управления доступом условно разделяются на два типа:

- агенты, обеспечивающие безопасность операционных систем семейства Windows, на которых размещены виртуальные инфраструктуры различных производителей (отображают информацию во вкладке «Агенты Windows», см. «Консоль»);
- агенты, обеспечивающие безопасность виртуальных инфраструктур (отображают информацию во вкладке «Агенты ВИ», см. «Консоль»).

Поддерживаемые платформы виртуализации (VMware vSphere, Microsoft Hyper-V, KVM, oVirt, zVirt, HOSTVM, РЕД Виртуализация) различаются количеством и типами элементов ВИ, но в общем случае обязательно включают в себя гипервизор и систему управления гипервизором. В состав СЗИ ВИ Dallas Lock входят специализированные АУД для каждой из поддерживаемых платформ виртуализации, их развертывание описано в соответствующих подразделах.

2.1 Требования к аппаратному и программному обеспечению

Для установки Центра управления СЗИ ВИ Dallas Lock минимальная и оптимальная конфигурация определяется требованиями к версии операционной системы Windows. Поддерживаются следующие версии ОС (64-bit):

- Windows 7 (SP 1) (Ultimate, Enterprise, Professional, Home Premium, Home Basic, Starter);
- Windows Server 2008 R2 (SP 1) (Foundation, Standard, Web, Enterprise, Datacenter);
- Windows 8 (Pro, Enterprise);
- Windows Server 2012 (Foundation, Essentials, Standard, Datacenter);
- Windows 8.1 (Pro, Enterprise);
- Windows Server 2012 R2 (Foundation, Essentials, Standard, Datacenter);
- Windows 10 (Enterprise, Education, Pro, Home);
- Windows 11 (Enterprise, Education, Pro, Home);
- Windows Server 2016 (Multipoint Premium Server, Essentials, Standard, Datacenter, Storage Server, Hyper-V Server);
- Windows Server 2019 (Essentials, Standard, Datacenter);
- Windows Server 2022 (Essentials, Standard, Datacenter).

Внимание! При использовании ОС Windows необходимо убедиться, что сервер telnet выключен.

Для установки агента DL vCenter for Windows ТС с установленным VMware vCenter Server 6.0/6.5/6.7 должно иметь следующий состав и характеристики программно-технического обеспечения:

1. Поддерживаемые ОС (64-bit):
   - Windows Server 2008 R2 (Foundation, Standard, Enterprise, Datacenter, Web Server 2008, Storage Server 2008);
   - Windows Server 2008 R2 (SP 1) (Foundation, Standard, Web, Enterprise, Datacenter);
   - Windows Server 2012 (Foundation, Essentials, Standard, Datacenter);
   - Windows Server 2012 R2 (Foundation, Essentials, Standard, Datacenter);
   - Windows Server 2016 (Essentials, Standard, Datacenter).
2. Минимальная комплектация:
   - процессор: Intel или AMD с 2-мя логическими ядрами по 2 ГГц каждое;
   - ОЗУ – минимум 12 Гб;
   - ПЗУ – минимум 60 Гб;
   - сетевая карта.

Для установки агента DL ESXi ТС с установленными VMware ESXi 6.0/6.5/6.7/7.0 должно иметь следующий состав и характеристики программно-технического обеспечения (минимальная комплектация):

- процессор: Intel или AMD с 2-мя логическими ядрами по 2 ГГц каждое, только x64;
- ОЗУ – минимум 8 Гб;
- ПЗУ – минимум 60 Гб;
- сетевая карта.

Для установки агента DL vCSA ТС с установленным vCSA 6.5/6.7/7.0 должно иметь следующий состав и характеристики программно-технического обеспечения:

- процессор: Intel или AMD с 2-мя логическими ядрами по 2 ГГц каждое, только x64;
- ОЗУ – минимум 12 Гб;
- ПЗУ – более 350 Гб;
- сетевая карта.

Полный список поддерживаемых платформ, процессоров, сетевых адаптеров и систем хранения доступен по ссылке: https://www.vmware.com/resources/compatibility/search.php.

Для установки агента DL Hyper-V ТС с установленным Windows Server (Hyper-V) (версий 2012, 2012 R2, 2016, 2019) 64-bit должно иметь следующий состав и характеристики программно-технического обеспечения:

- процессор: Intel или AMD с 2-мя логическими ядрами по 2 ГГц каждое;
- ОЗУ – минимум 2 Гб;
- ПЗУ – минимум 32 Гб;
- сетевая карта.

Для установки агента DL KVM ТС с установленным гипервизором KVM должно иметь следующий состав и характеристики программно-технического обеспечения:

1. Поддерживаемые ОС:
   - Astra Linux 1.6;
   - Astra Linux 2.12;
   - CentOS 7.5;
   - Linux Mint 18.3;
   - Ubuntu 18.04.2 LTS;
2. Минимальная комплектация:
   - процессор: Intel или AMD с 2-мя логическими ядрами по 2 ГГц каждое;
   - ОЗУ – минимум 1 Гб;
   - ПЗУ – минимум 10 Гб;
   - сетевая карта.

Внимание! Для установки агента DL Engine и DL Host инфраструктура, построенная на базе oVirt/zVirt/HOSTVM и РедВиртуализации должна быть развернута только в вариантах, предусмотренных документацией изготовителя - self-hosted и standalone.

Для установки агента DL Engine ТС с установленной системой управления виртуализацией oVirt (версия 4.4.x) должно иметь следующий состав и характеристики программно-технического обеспечения соответственно:

1. Поддерживаемые ОС:
   - oVirt Node.
2. Минимальная конфигурация:
   - процессор: Intel или AMD с 2-мя логическими ядрами по 2 ГГц каждое;
   - ОЗУ – минимум 4 Гб;
   - ПЗУ – минимум 25 Гб;
   - сетевая карта – минимум 1 Гбит/с.

Для установки агента DL Host ТС с установленным гипервизором oVirt (версия 4.4.x) должно иметь следующий состав и характеристики программно-технического обеспечения соответственно:

1. Поддерживаемые ОС:
   - oVirt Node.
2. Минимальная комплектация:
   - процессор: Intel или AMD с 2-мя логическими ядрами по 2 ГГц каждое;
   - ОЗУ – минимум 2 Гб;
   - ПЗУ – минимум 64 Гб;

- сетевая карта – минимум 1 Гбит/с.

Для установки агента DL Engine TC с установленной системой управления виртуализацией zVirt (версий 3.0, 3.1) должно иметь следующий состав и характеристики программно-технического обеспечения соответственно:

1. Поддерживаемые ОС:
   - zVirt Node.
2. Минимальная конфигурация:
   - процессор: двухъядерный x86-64 с поддержкой VT-x/AMD-V;
   - ОЗУ – минимум 4 Гб;
   - ПЗУ – минимум 94 Гб;
   - сетевая карта – минимум 1 Гбит/с.

Для установки агента DL Host TC с установленным гипервизором zVirt (версий 3.0, 3.1) должно иметь следующий состав и характеристики программно-технического обеспечения соответственно:

1. Поддерживаемые ОС:
   - zVirt Node.
2. Минимальная комплектация:
   - процессор: двухъядерный x86-64 с поддержкой VT-x/AMD-V;
   - ОЗУ – минимум 4 Гб;
   - ПЗУ – минимум 94 Гб;

сетевая карта – минимум 1 Гбит/с.

Для установки агента DL Engine TC с установленной системой управления виртуализацией HOSTVM должно иметь следующий состав и характеристики программно-технического обеспечения соответственно:

1. Поддерживаемые ОС:
   - HOSTVM Node.
2. Минимальная конфигурация:
   - процессор: Intel или AMD с 2-мя логическими ядрами по 2 ГГц каждое;
   - ОЗУ – минимум 4 Гб;
   - ПЗУ – минимум 25 Гб;
   - сетевая карта – минимум 1 Гбит/с.

Для установки агента DL Host TC с установленным гипервизором HOSTVM должно иметь следующий состав и характеристики программно-технического обеспечения соответственно:

1. Поддерживаемые ОС:
   - HOSTVM Node.
2. Минимальная комплектация:
   - процессор: Intel или AMD с 2-мя логическими ядрами по 2 ГГц каждое;
   - ОЗУ – минимум 2 Гб;
   - ПЗУ – минимум 64 Гб;
   - сетевая карта – минимум 1 Гбит/с.

Для установки агента DL Engine TC с установленной системой управления виртуализацией РедВиртуализация 7.3 должно иметь следующий состав и характеристики программно-технического обеспечения соответственно:

1. Поддерживаемые ОС:
   - RED OS MUROM 7.3.1.
2. Минимальная конфигурация:
   - процессор: Intel или AMD с 2-мя логическими ядрами;
   - ОЗУ – минимум 16 Гб;
   - ПЗУ – минимум 80 Гб;
   - сетевая карта – минимум 1 Гбит/с.

Для установки агента DL Host TC с установленным гипервизором РедВиртуализация 7.3 должно иметь следующий состав и характеристики программно-технического обеспечения соответственно:

1. Поддерживаемые ОС:
   - RED OS MUROM 7.3.1.
2. Минимальная комплектация:
   - процессор: Intel или AMD с 2-мя логическими ядрами;
   - ОЗУ – минимум 16 Гб;
   - ПЗУ – минимум 80 Гб;

- сетевая карта – минимум 1 Гбит/с.

Веб-интерфейс СЗИ ВИ корректно отображается в следующих веб-браузерах:

- Chrome 91.0.X;
- Firefox 89.0.2;
- Edge 91.0.X;
- Яндекс.Браузер 21.3.3;
- Safari 14.4;
- Спутник 5.3.X (Windows, Linux);
- Chromium-gost 91.0.X;

Для установки компонентов СЗИ ВИ необходимо минимум 1 Гб свободного дискового пространства на системном разделе жесткого диска.
Для использования СЗИ ВИ необходимо настроить сетевой протокол TCP/IP.
Требуется наличие USB-порта в аппаратной части ЦУ СЗИ ВИ для использования аппаратного идентификатора.

ТС с установленной Консолью должно иметь в составе аппаратный идентификатор (eToken или Рутокен (Rutoken)), содержащий лицензионный ключ для изделия СЗИ ВИ Dallas Lock.

2.2 Ограничения при установке и эксплуатации

СЗИ ВИ Dallas Lock редакции «Стандартная» и «Расширенная» имеют следующие ограничения по эксплуатации:

1. **СЗИ ВИ:**
   1) При наличии на компьютере нескольких жестких дисков, операционная система должна быть установлена на первый жесткий диск.
   2) На компьютерах, на которых будет производиться установка компонентов Центра управления СЗИ ВИ Dallas Lock, агента DL vCenter for Windows и агента DL Hyper-V необходимо убедиться, что в BIOS отключена функция Secure Boot.
   3) При наличии на жестком диске нескольких разделов, операционная система должна быть установлена на диск C.
   4) Установка компонентов СЗИ ВИ всегда производится в каталог «C:\DLVI».
   5) На время установки и удаления СЗИ ВИ необходимо отключить программные антивирусные средства, а при возникновении ошибок, необходимо удалить антивирусные средства на время установки и удаления СЗИ ВИ.
   6) Не поддерживается установка компонента «Центр управления СЗИ ВИ Dallas Lock» на ПК с ОС Windows Server 2008 R2 (SP 1), 2012, 2012 R2, 2016 или 2019, установленной в режиме «Server Core».
   7) При обновлении ОС Windows (до Windows 8, Windows 8.1, Windows 10, Windows 11) изделие необходимо удалить (см. п. 2.9 «Удаление СЗИ ВИ»), выполнить обновление, после чего установить изделие, используя при необходимости функцию сохранения конфигурации (см. п. 11.1 «Сохранение конфигурации ЦУ СЗИ ВИ»).
   8) Устанавливать компоненты СЗИ ВИ на компьютер может только пользователь, обладающий правами администратора на данном компьютере. Это может быть локальный или доменный пользователь. Локальную установку необходимо выполнять только из-под сессии текущего авторизованного пользователя. Запуск установки от имени другого пользователя (Run as) не допускается. Для корректной работы СЗИ ВИ с AD, установка компонентов защиты должна осуществляться из-под УЗ пользователя, обладающего необходимыми правами для работы со средой виртуализации.
   9) Суперпользователь (root, администратор среды виртуализации) и пользователи с аналогичными правами обладают привилегиями, с помощью которых могут внести изменения в СЗИ ВИ и ее настройки, способные нарушить корректность выполнения функций СЗИ ВИ вплоть до ее неработоспособности. Контроль привилегированных пользователей должен осуществляться посредством применения организационных мер защиты.
   10) Имя и пароль пользователя для входа в операционную систему, выполнившего установку, автоматически становятся именем и паролем для первого входа на компьютер с установленным СЗИ ВИ, пользователем в качестве суперадминистратора. Если же компьютер является клиентом контроллера домена, и при установке использовалась конфигурация по умолчанию[3], то зайти на защищенный компьютер

[3] Подробнее в п.11.1 «Сохранение конфигурации ЦУ СЗИ ВИ».

можно под любым доменным пользователем, так как в СЗИ ВИ автоматически создается и регистрируется учетная запись «**»[4].

11) При использовании ОС Windows необходимо убедиться, что сервер telnet выключен.
12) Для настройки SQL и других серверов БД может потребоваться дополнительная настройка сессий исключений на Сервере УД (подробнее см. в документе «Инструкция по использованию SQL-сервера для СЗИ ВИ Dallas Lock» ПФНА.501410.001 И3).
13) Необходимо периодически проводить проверку контроля целостности образов виртуальных машин[5]. Для проведения необходимо на уровне гипервизора в категории «Состояние» → «Контроль целостности» → «Конфигурации ВМ» выбрать ВМ и нажать кнопку «Проверить» (подробнее см. п. 7.1 «Контроль целостности файлов»).
14) При установке СЗИ ВИ требуется скачивание пакетов из глобальной сети. Для автономных компьютеров, не подключенных к глобальной сети, необходимо, чтобы в локальной сети был расположен официальный репозиторий соответствующего дистрибутива ОС и были выполнены соответствующие настройки инфраструктуры. Следует обратить внимание, что корректная работа СЗИ ВИ гарантируется только с официальными репозиториями, подключение к которым осуществляется сразу после установки ОС.
15) При наделении пользователя правом на изменение системной даты и времени, а также смену часового пояса, у пользователей появляется возможность обхода санкционированного времени работы.

2. vSphere:

1) Установка платформы виртуализации VMware vSphere всегда должна производиться по пути, который предлагается инсталлятором платформы по умолчанию. В случае выбора любого другого каталога для установки, при инсталляции СЗИ ВИ произойдет ошибка копирования файлов и система не будет установлена.
2) Если будут использоваться сторонние firewall-программы, то необходимо добавить разрешения для TCP портов 80, 443, 514, 8080, 11120, 15090, 17491, 17492, 17493, 17495, 17497, 11111 в их настройках вручную и убедиться, что открыты порты, необходимые для работы компонентов VMware vSphere, а также для иного используемого стороннего программного обеспечения (подробнее о добавлении разрешений см. п. 6.3 «Удаленный доступ к СВ».
3) В VMware ESXi 6.7 по умолчанию включен режим Secure Boot. Перед установкой агента DL vCSA на гипервизор данный режим необходимо отключить в настройках виртуальной машины.
4) ЦУ СЗИ ВИ не осуществляет контроль пользователей доменной группы «ESX Admins», использующейся для авторизации доменных пользователей на гипервизорах ESXi, введенных в домен AD. В группу AD «ESX Admins» следует включать только высоко доверенных пользователей.
5) Перед установкой агента DL vCSA необходимо проверить срок действия пароля root. При истекшем сроке действия пароля root для vCSA установка агента DL vCSA не будет осуществлена.
6) В случае, если IP-адрес сервера виртуализации vCSA является динамическим, его DNS-имя не должно содержать кириллические символы.
7) Перед установкой агента DL ESXi рекомендуется выполнить настройку кластеров и их состава. В противном случае, после ввода (вывода) гипервизора в (из) состав(а) кластера или папки, необходимо снова установить учетные данные гипервизора. Далее, либо переустановить агента DL ESXi, либо перезагрузить его командой "/etc/init.d/confident-agentd restart" и выполнить настройку гипервизора в Консоли.
8) Перед установкой агента DL ESXi необходимо убедиться, что на гипервизоре ESXi есть сконфигурированный VMFS раздел (Datastore).
9) Установка агента DL ESXi не допускается на гипервизор ESXi с папкой scratch, находящейся на RAM диске (/tmp/scratch).
10) Перед удалением гипервизора ESXi из vCenter необходимо выполнить удаление агента DL ESXi с данного гипервизора ESXi.
11) При обновлении гипервизора ESXi необходимо удалить агент DL ESXi, выполнить обновление, после чего установить агент DL ESXi.
12) В штатном режиме функционирования СЗИ ВИ запрещается использовать локальный вход на СВ vCSA. Возможность настройки среды виртуализации через локальную

[4] Подробнее в п. 5.1.2.3 «Регистрация доменных учетных записей по маске».

[5] Периодический контроль целостности образа виртуальной машины определяется в рамках действующих положений ИБ по организации, в котором указывается период выполнения ручной проверки КС.

консоль определяется включением параметра «[vCSA] Вход: разрешить локальный вход с консоли» и является конфигурационным режимом работы СЗИ ВИ, необходимым для конфигурирования виртуальной инфраструктуры.

13) Не допускается использование СЗИ ВИ на компьютерах, введенных в домен AD с зарезервированным именем «vsphere.common».
14) При установке VMware vCenter/vCSA не допускается использовать имя «vsphere.common» для домена SSO (Single Sign-On).

3. Hyper-V:

1) Перед установкой Центра управления СЗИ ВИ Dallas Lock и агента DL Hyper-V необходимо убедиться, что на компьютерах, на которых будет производиться установка данных компонентов, в BIOS отключена функция Secure Boot.
2) СЗИ ВИ «Dallas Lock» поддерживает управление серверами Hyper-V через System Center Virtual Machine Manager и Failover Cluster Manager, при этом следует учитывать, что в режиме использования данных инструментов управления кластеризацией типовые операции могут отличаться от выполняемых операций, вызванных через Консоль ЦУ СЗИ ВИ.

4. KVM/oVirt/zVirt/HOSTVM/РЕД Вирт:

1) При обновлении гипервизора KVM необходимо удалить агент DL KVM, выполнить обновление, после чего установить агент DL KVM.
2) При работе с KVM в консоли СЗИ ВИ недоступны к управлению и не отображаются ВМ пользователей (доступны только qemu:///system). Для создания и использования ВМ пользователей необходимо выключить политику «Libvirt: Блокировать запуск ВМ в пространстве пользователя» (см. п. 5.3.1.3 «Параметры входа для KVM/oVirt/zVirt/HOSTVM»).
3) Для корректной работы агента DL Engine требуется наличие python версии не ниже 3.6.
4) Для предоставления доступа пользователю к управлению ВМ необходимо добавить данного пользователя в следующие группы:
   - Для ОС Linux Mint – libvirt.
   - Для ОС Ubuntu – libvirt, kvm.
   - Для ОС Astra Linux (Орел 2.12) – kvm, libvirt, libvirt-qemu.
   - Для ОС Astra Linux (Смоленск 1.6) – kvm, libvirt, libvirt-qemu, libvirt-admin.
   - Для ОС CentOS – kvm.
5) Рекомендуется перед добавлением инфраструктуры oVirt/zVirt/HOSTVM/РЕД Виртуализация в ДБ СЗИ ВИ завести встроенные учетные записи (internal) и доменные учетные записи для использования их при работе с виртуальной инфраструктурой.
6) При работе с платформами виртуализации oVirt/zVirt/РЕД Виртуализации поддерживаются только конфигурации Standalone и Self-hosted.
7) При работе с платформой виртуализации HOSTVM поддерживается только конфигурации Self-hosted.
8) При обновлении СВ oVirt необходимо удалить агент DL Engine, выполнить обновление, после чего установить агент DL Engine.
9) При обновлении гипервизора oVirt необходимо удалить агент DL Host, выполнить обновление, после чего установить агент DL Host.
10) При обновлении СВ zVirt необходимо удалить агент DL Engine, выполнить обновление, после чего установить агент DL Engine.
11) При обновлении гипервизора zVirt необходимо удалить агент DL Host, выполнить обновление, после чего установить агент DL Host.
12) При обновлении СВ HOSTVM необходимо удалить агент DL Engine, выполнить обновление, после чего установить агент DL Engine.
13) При обновлении гипервизора HOSTVM необходимо удалить агент DL Host, выполнить обновление, после чего установить агент DL Host.
14) При обновлении СВ РЕД Вирт необходимо удалить агент DL Engine, выполнить обновление, после чего установить агент DL Engine.
15) При обновлении гипервизора РЕД Вирт необходимо удалить агент DL Host, выполнить обновление, после чего установить агент DL Host.

2.2.1 Различие редакций СЗИ ВИ

СЗИ ВИ Dallas Lock редакции «Расширенная» имеет следующие преимущества в функциональных возможностях:

1. Для Microsoft Hyper-V присутствует:
- поддержка High Availability (HA);

- контроль управления через Failover Cluster Manager;
- контроль управления через System Center Virtual Machine Manager.

2. Для VMware vSphere присутствует поддержка:
   - Platform Services Controller (PSC);
   - vCenter High Availability;
   - VMware Fault Tolerance;
   - Enhanced Linked Mode;
   - Embedded Linked Mode;
   - Hybrid Linked Mode.
3. Для Консоли ЦУ СЗИ ВИ присутствует:
   - Инфографика (построение диаграмм событий НСД).

2.3 Порядок развертывания компонентов

2.3.1 Порядок развертывания СЗИ ВИ для VMware vSphere vCenter

Развертывание СЗИ ВИ рекомендуется проводить в следующем порядке.

№ п/п	Шаг развертывания	Описание
1	Установить Центр управления СЗИ ВИ Dallas Lock на компьютер, предназначенный для ЦУ СЗИ ВИ	см. раздел 2.5.1
2	Установить агент DL vCenter for Windows на сервер виртуализации	см. раздел 2.5.2.2 или 2.6.1.2
3	Ввести сервер виртуализации в домен безопасности	см. раздел 2.5.2.3 или 2.6.1.2
4	Установить агент DL ESXi на гипервизор ESXi	см. раздел 2.5.2.4

2.3.2 Порядок развертывания СЗИ ВИ для VMware vSphere vCSA

№ п/п	Шаг развертывания	Описание
1	Установить Центр управления СЗИ ВИ Dallas Lock на компьютер, предназначенный для ЦУ СЗИ ВИ	см. раздел 2.5.1
2	Установить агент DL vCSA и ввести в домен безопасности сервера виртуализации vCSA	см. раздел 2.5.3.2 или 2.6.2.2
3	Установить агент DL ESXi на гипервизор ESXi	см. раздел 2.5.2.4

2.3.3 Порядок развертывания СЗИ ВИ для Hyper-V

№ п/п	Шаг развертывания	Описание
1	Установить Центр управления СЗИ ВИ Dallas Lock на компьютер, предназначенный для ЦУ СЗИ ВИ	см. раздел 2.5.1
2	Установить агент DL Hyper-V	см. раздел 2.5.4.2
3	Ввести сервер виртуализации в домен безопасности	см. раздел 2.5.4.3 или 2.6.3.2

2.3.4 Порядок развертывания СЗИ ВИ для KVM

№ п/п	Шаг развертывания	Описание
1	Установить Центр управления СЗИ ВИ Dallas Lock на компьютер, предназначенный для ЦУ СЗИ ВИ	см. раздел 2.5.1
2	Установить агент DL KVM	см. раздел 2.5.5.2 или 2.6.4.2
3	Ввести сервер виртуализации в домен безопасности	см. раздел 2.5.5.2 или 2.6.4.2

2.3.5 Порядок развертывания СЗИ ВИ для oVirt/zVirt/HOSTVM/РЕД Вирт

№ п/п	Шаг развертывания	Описание
1	Установить Центр управления СЗИ ВИ Dallas Lock на компьютер, предназначенный для ЦУ СЗИ ВИ	см. раздел 2.5.1
2	Установить агент DL Engine	см. раздел 2.5.6.2 или 2.6.5.2
3	Ввести сервер виртуализации в домен безопасности	см. раздел 2.5.6.2 или 2.6.5.2
4	Установить агент DL Host на гипервизор oVirt/zVirt/HOSTVM/РЕД Вирт	см. раздел 2.5.6.3

2.4 Подготовка к установке СЗИ ВИ

2.4.1 Предварительная подготовка

Перед развертыванием СЗИ ВИ необходимо выполнить следующие действия:

1. Если в BIOS компьютера включена антивирусная защита, то на время установки ее необходимо отключить.
2. Если на компьютере уже установлена система защиты, ее необходимо удалить.
3. Проверить состояние жестких дисков компьютера, например, при помощи приложения chkdsk.exe или служебной программы проверки диска из состава ОС Windows, и устранить выявленные дефекты.
4. Рекомендуется произвести дефрагментацию жесткого диска.
5. Необходимо убедиться, что на диске C:\ имеется необходимое свободное пространство для установки системы защиты.
6. Проверить компьютер на отсутствие вирусов.
7. Проверить корректность установленной даты и времени на всех компонентах среды виртуализации.
8. Перед установкой системы защиты необходимо выгрузить из памяти все резидентные антивирусы.
9. Закрыть все запущенные приложения, так как установка системы потребует принудительной перезагрузки.
10. Установить пакет .NET Framework 4.5 (поставляется на диске с изделием) в случае отсутствия в ОС.
11. Должен быть установлен пакет Aladdin eToken PKI Client (драйвер для USB-ключей Rutoken) на ПК, предназначенный для ЦУ СЗИ ВИ.
12. Конфигурацию протоколов TLS на серверах vCenter и хостах ESXi необходимо производить штатной утилитой VMware перед развертыванием СЗИ ВИ.
13. Войти на компьютер с учетной записи администратора, под которой производилась установка VMware vSphere (первичный администратор) при локальной установке агента DL vCenter.

14. Проверить актуальность паролей для VMware vCenter (for Windows и vCSA) для учетных записей administrator@vsphere.local и root и срока их действия.
15. Перед установкой Центра управления СЗИ ВИ Dallas Lock, агента DL vCenter for Windows и агента DL Hyper-V необходимо убедиться, что на компьютерах, на которых будет производиться установка данных компонентов, в BIOS отключена функция Secure Boot.

Также рекомендуется отключить кэширование записи для всех дисков. Для отключения кэширования записи необходимо:

1. Открыть Диспетчер устройств на компьютере.
2. Выбрать в узле дерева «Дисковые устройства» диск, в его контекстном меню выбрать пункт «Свойства» и в появившемся диалоге открыть вкладку «Политика».
3. Снять флаг в поле «Разрешить кэширование записи на диск» («Включить кэширование записи»).
4. Нажать кнопку «ОК».
5. Повторить вышеуказанные действия для всех дисков.

Примечание. Если используется RAID-контроллер, то, возможно, в BIOS контроллера нужно включить режим эмуляции «int13». Кроме того, на многих системных платах, имеющих встроенный RAID-контроллер, можно выбрать режим работы этого контроллера «Native» или «RAID». Рекомендуется использовать режим «Native». Необходимо использовать эти режимы с осторожностью, так как их переключение влияет на работу ОС.

2.4.2 Особенности установки

Внимание! Устанавливать компоненты СЗИ ВИ на компьютер может только пользователь, обладающий правами администратора на данном компьютере. Это может быть локальный или доменный пользователь.

Локальную установку необходимо выполнять только из-под сессии текущего авторизованного пользователя. Запуск установки от имени другого пользователя (Run as) не допускается.

Примечание. Если установка производится под учетной записью доменного пользователя:

1. Важно, чтобы он был добавлен в группу «Администраторы».
2. Необходимо, чтобы именно под этой учетной записью была произведена установка VMware vSphere (первичный администратор) при локальной установке агента DL vCenter.
3. Необходимо, чтобы установка агента DL Hyper-V и ввод в ДБ СЗИ ВИ при работе с кластерами Hyper-V осуществлялся под учетной записью администратора домена.
4. В процессе эксплуатации СЗИ ВИ необходимо зарегистрировать в СЗИ ВИ хотя бы одну учетную запись локального пользователя с правами администратора, так как при возможном выводе компьютера из домена, вход под доменной учетной записью будет невозможен.

Пользователь, установивший систему защиты, автоматически становится привилегированным пользователем – **суперадминистратором.** Необходимо запомнить имя и пароль этого пользователя, так как некоторые операции можно выполнить только из-под его учетной записи. Изменять учетную запись суперадминистратора средствами Windows запрещено.

Внимание! Имя и пароль пользователя для входа в операционную систему, выполнившего установку, автоматически становятся именем и паролем для первого входа на компьютер с установленным СЗИ ВИ, пользователем в качестве суперадминистратора.

Если же компьютер является клиентом контроллера домена, и при установке использовалась конфигурация по умолчанию[6], то зайти на защищенный компьютер можно под любым доменным пользователем, так как в СЗИ ВИ автоматически создается и регистрируется учетная запись «**»[7].

[6] Подробнее в п.11.1 «Сохранение конфигурации ЦУ СЗИ ВИ».

[7] Подробнее в п. 5.1.2.3 «Регистрация доменных учетных записей по маске».

Примечание. В процессе установки СЗИ ВИ будет произведена автоматическая настройка брандмауэра Windows (Windows Firewall).

Внимание! Если будут использоваться сторонние firewall-программы, то необходимо добавить разрешения для TCP портов 80, 443, 514, 8080, 17491, 17492, 17493, 17495, 17497, 11111 в их настройках вручную и убедиться, что открыты порты, необходимые для работы компонентов VMware vSphere, а также для иного используемого стороннего программного обеспечения (подробнее о добавлении разрешений см. п. 6.3 «Удаленный доступ к СВ».

Примечание. При вводе гипервизора ESXi в домен AD после установки агента СЗИ ВИ и установки учетных данных с Консоли ЦУ СЗИ ВИ требуется повторно провести установку учетных данных штатным способом (см. п. 2.5.2.4 «Установка и удаление агента DL ESXi на гипервизоре ESXi»).

Внимание! ЦУ СЗИ ВИ не осуществляет контроль пользователей доменной группы «ESX Admins», использующейся для авторизации доменных пользователей на гипервизорах ESXi, введенных в домен AD. В группу AD «ESX Admins» следует включать только высоко доверенных пользователей.

Примечание. При возникновении нештатной ситуации в процессе установки СЗИ ВИ для более оперативной помощи от технической поддержки можно сформировать файлы с расширенными логами (подробнее см. п. 11.2 «Работа с логами»).

2.5 Развертывание СЗИ ВИ

С помощью инсталлятора СЗИ ВИ Dallas Lock производится локальная установка следующих компонентов:

- Центр управления СЗИ ВИ Dallas Lock;
- агент DL vCenter for Windows;
- агент DL Hyper-V/SC VMM.

2.5.1 Установка компонента «Центр управления СЗИ ВИ Dallas Lock»

Порядок установки компонента «Центр управления СЗИ ВИ Dallas Lock» аналогичен для всех платформ виртуализации:

1. Запустить установочный файл «DLVI.msi» (рис. 1), разрешить установку программного обеспечения СЗИ ВИ на компьютер (рис. 2) и дождаться завершения настройки Windows СЗИ ВИ Dallas Lock. ЦУ СЗИ ВИ всегда по умолчанию устанавливается в папку «C:\DLVI\DlSecServer».

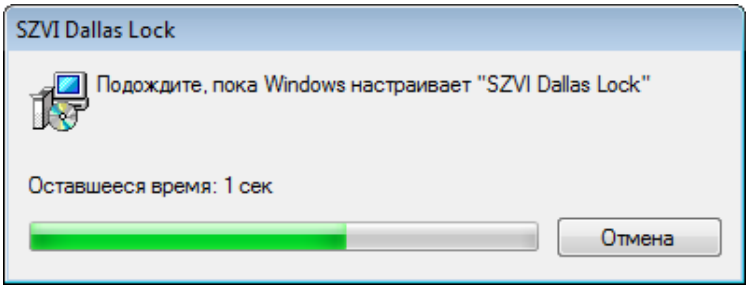


Рис. 1 – Процесс запуска установочного файла

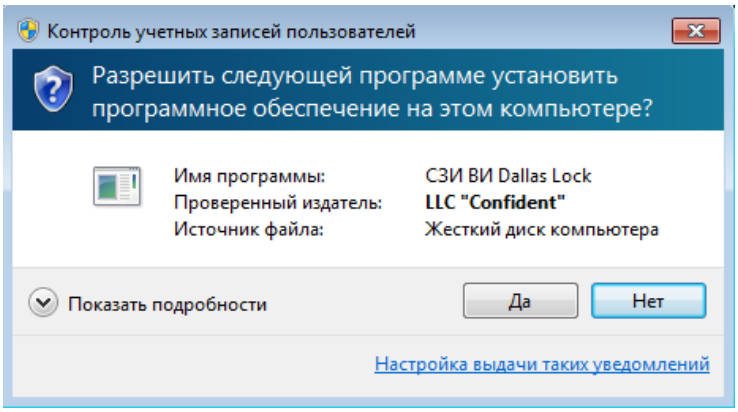


Рис. 2 – Разрешение на установку программы в ОС

2. После завершения настройки запустится окно установщика (рис. 3), с помощью которого в программе установки необходимо выполнять действия по подсказкам программы. На каждом шаге установки предоставляется возможность полной отмены установки. Для этого служит кнопка «Отмена». Выполнение следующего шага установки выполняется с помощью кнопки «Далее». Для возврата на предыдущий шаг установки служит кнопка «Назад».

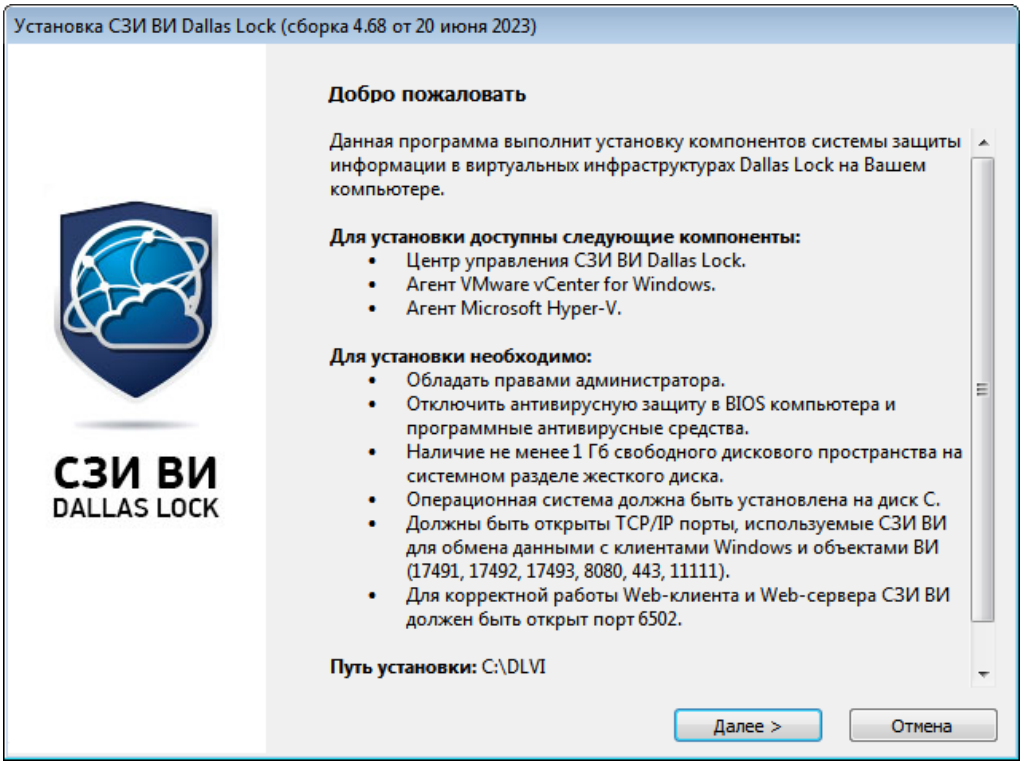


Рис. 3 – Окно начало установки СЗИ ВИ

Для продолжения установки нажать кнопку «Далее».

3. Ввести номер лицензии продукта. Код активации технической поддержки при желании можно будет ввести позже (см. п. 11.2 «Работа с логами») (рис. 4).

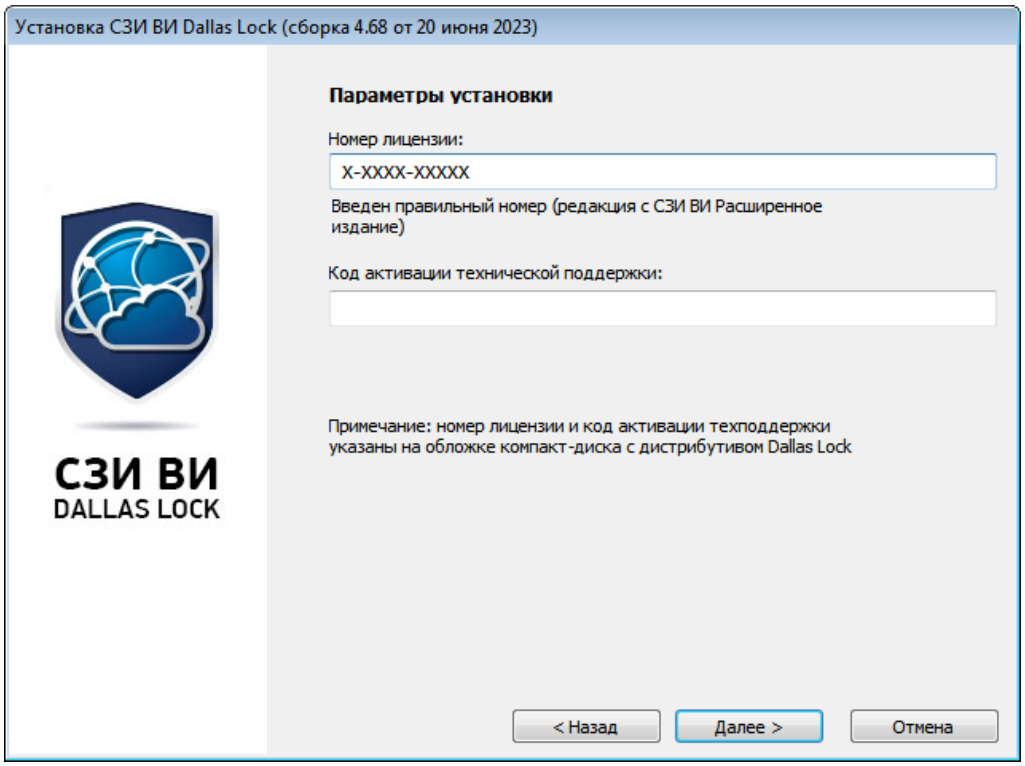


Рис. 4 – Ввод параметров установки

4. Выбрать компонент «Центр управления СЗИ ВИ Dallas Lock» (рис. 5), нажать кнопку «Далее».

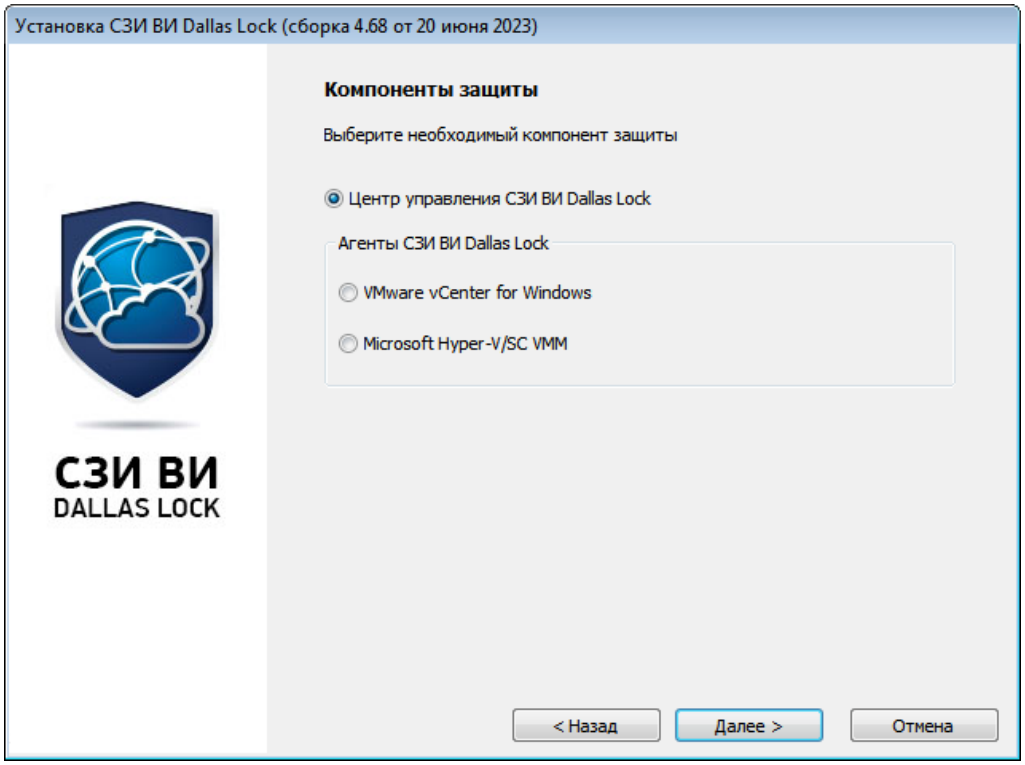


Рис. 5 – Выбор устанавливаемого компонента

5. Если необходимо, поставить флаг и заполнить поля подключения к системе хранения данных MS SQL Server (рис. 6) (подробнее см. в документе «Инструкция по использованию SQL-сервера для СЗИ ВИ Dallas Lock» ПФНА.501410.001 И3). Для продолжения установки нажать кнопку «Далее».

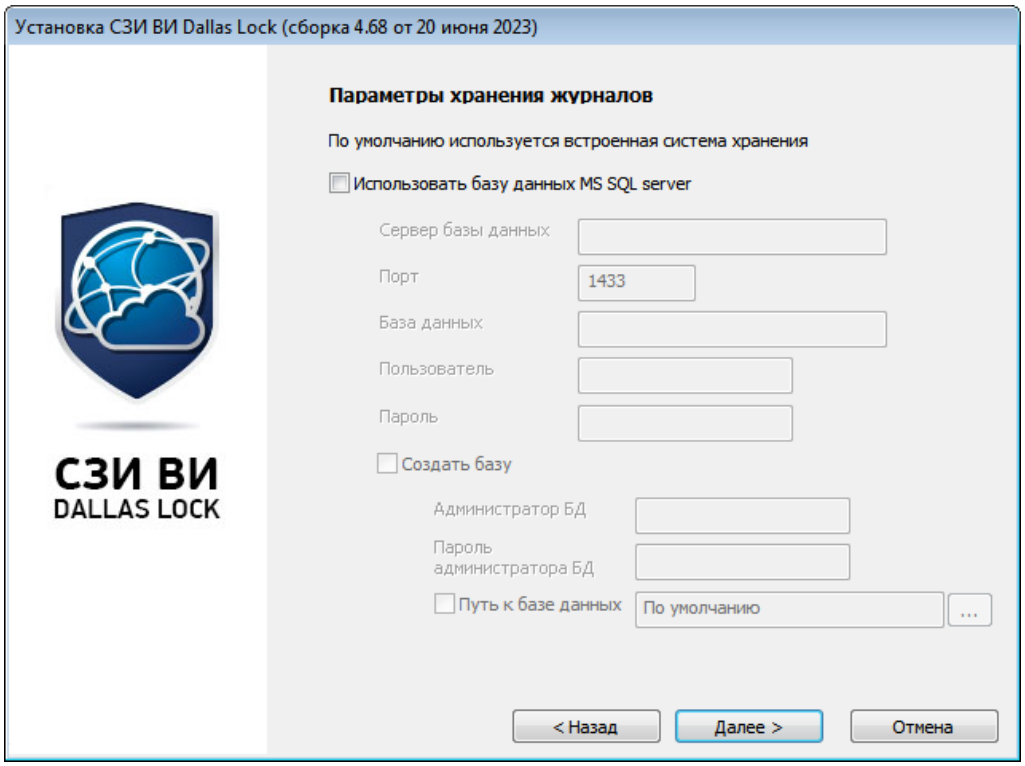


Рис. 6 – Ввод параметров БД MS SQL Server

6. Если необходимо, поставить флаг и заполнить поля подключения к Серверу лицензий (рис. 7) (подробнее об использовании Сервера лицензий см. в документе «Инструкция по использованию сервера лицензий» ПФНА.501410.001 И4). Для продолжения установки нажать кнопку «Установить».

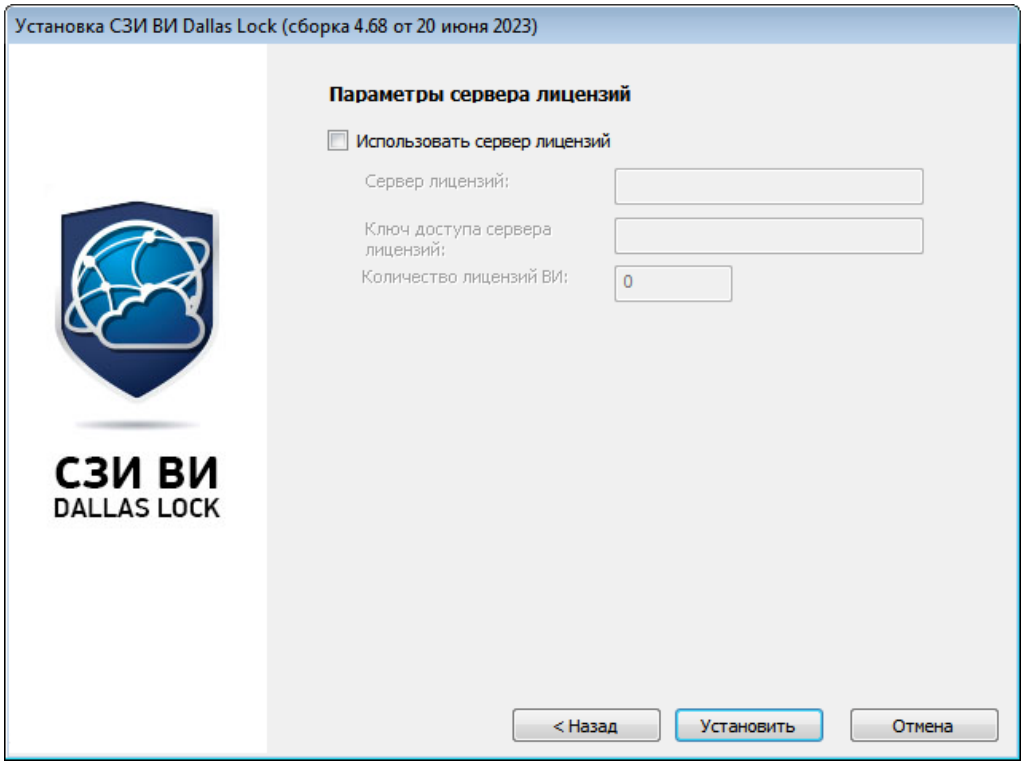


Рис. 7 – Ввод параметров сервера лицензий

7. Далее последует процесс установки. Если процесс прошел без ошибок, то для завершения установки требуется перезагрузка ПК. После нажатия кнопки «Перезагрузить» (рис. 8) появится уведомление о том, что через 1 минуту произойдет автоматическая перезагрузка ПК (рис. 9).

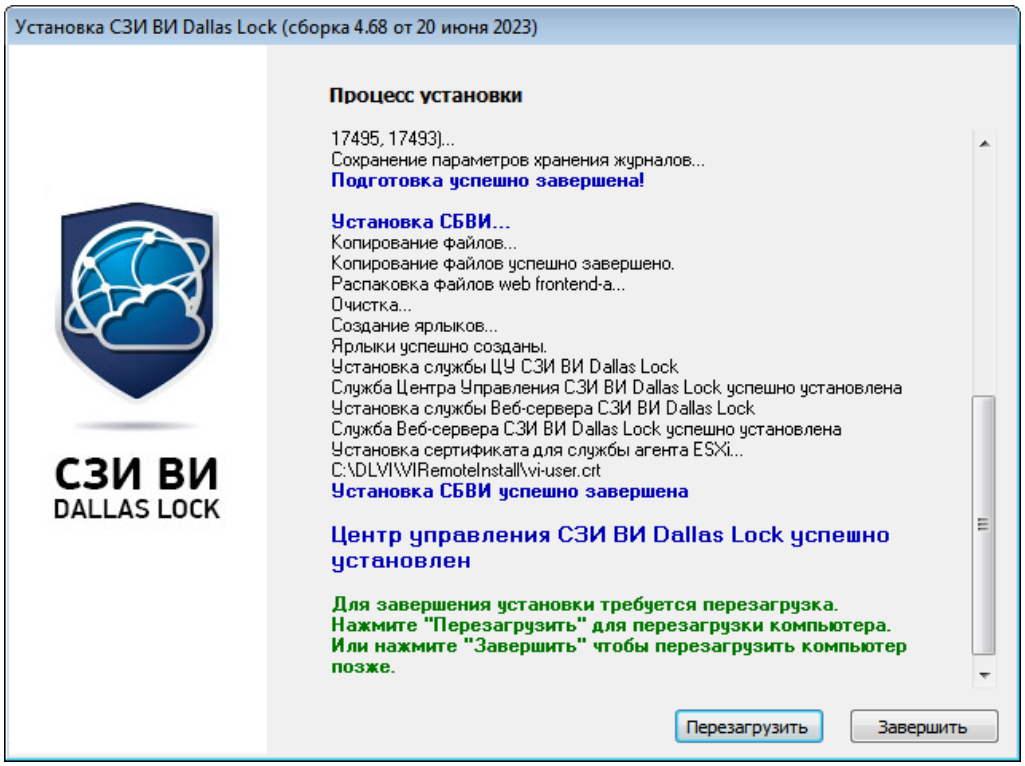


Рис. 8 – Завершение процедуры установки

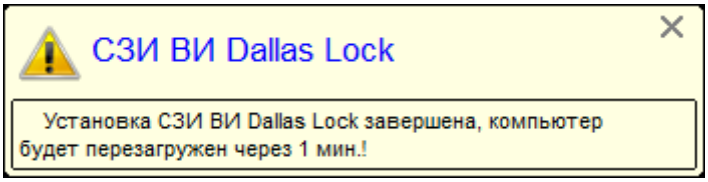


Рис. 9 – Уведомление о перезагрузке ПК

Если требуется выполнить перезагрузку позже, необходимо нажать кнопку «Завершить».

8. После перезагрузки ПК и входа на защищенный компьютер (см. п. 2.5.1.1 «Вход на защищенный компьютер с ОС Windows») необходимо пождать несколько секунд, пока загрузится служба СЗИ ВИ и только после этого запустить Консоль (подробнее см. п. 3.1 «Консоль»). Уведомление о том, что компьютер защищен СЗИ ВИ появляется только после первой перезагрузки (рис. 10).

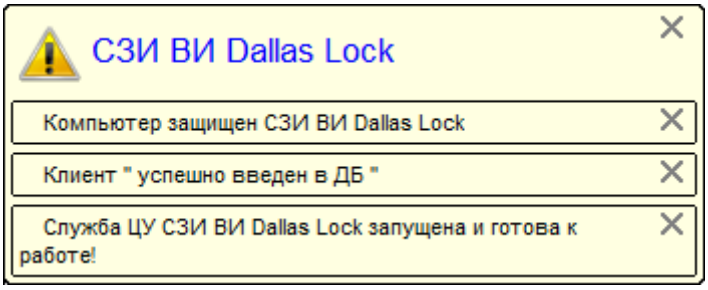


Рис. 10 – Уведомления о запущенной службе СЗИ ВИ

2.5.1.1 Вход на защищенный компьютер с ОС Windows

При загрузке компьютера с установленным на нем СЗИ ВИ, в зависимости от версии ОС Windows, появляется экран приветствия (приглашение на вход в систему) (рис. 11, рис. 12).

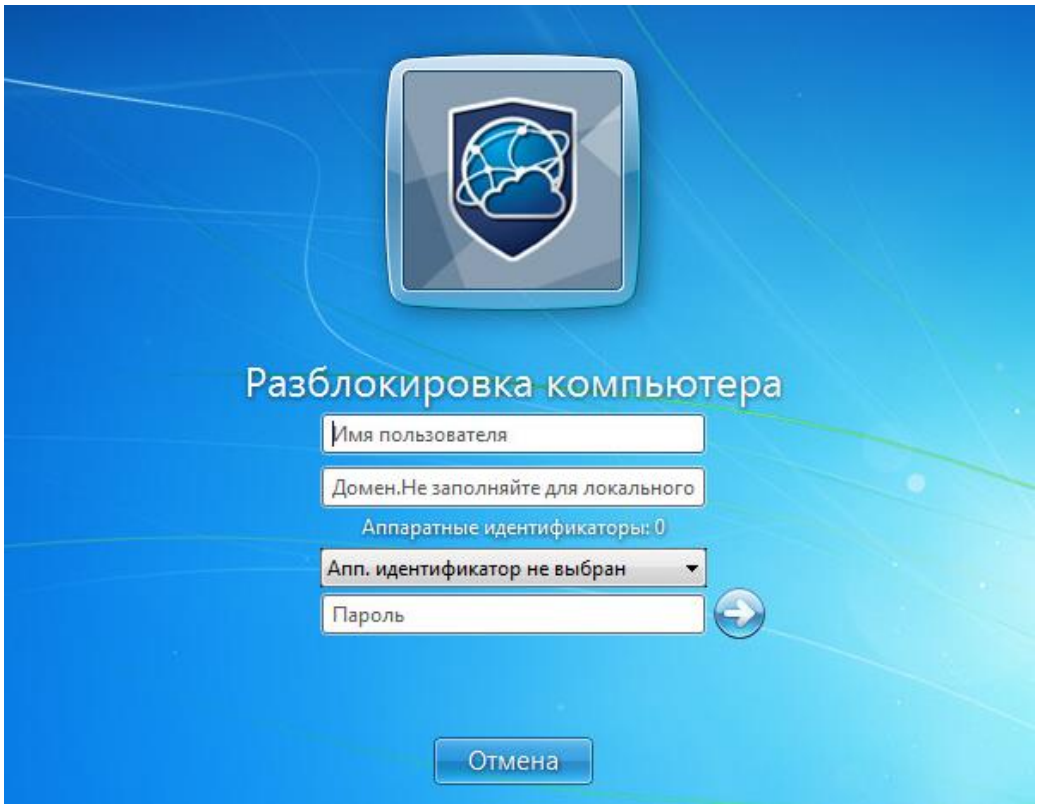


Рис. 11 – Экран приветствия в ОС Windows 7

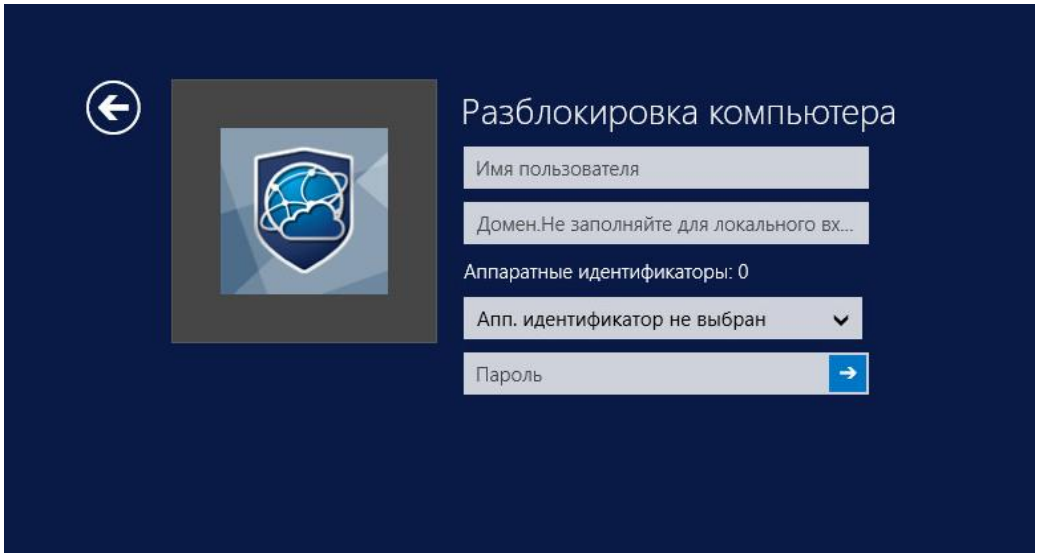


Рис. 12 – Экран приветствия ОС Windows Server 2012 R2

Для входа на компьютер с установленным на нем компонентом СЗИ ВИ каждому пользователю предлагается выполнить следующую последовательность шагов:

1. Заполнить поле имени пользователя, под которым он зарегистрирован в системе. В зависимости от настроек системы защиты в этом поле может оставаться имя пользователя, выполнившего вход последним.
2. Заполнить поле имени домена. Если пользователь доменный, то указывается имя домена, если пользователь локальный, то в этом поле оставляется имя компьютера или оставляется пустое значение.
3. Если пользователю назначен аппаратный идентификатор, то его необходимо предъявить (подробное описание приводится ниже). Подробнее настройки параметров входа и аппаратных идентификаторов приведены в п. 5.4 «Настройки параметров для клиентов Windows» и п. 5.4.4 «Настройка средств аппаратной идентификации», п. 5.5 «Аппаратная идентификация пользователя» соответственно.
4. Ввести пароль. Поле для ввода является текстовым. При вводе пароля происходит маскирование символов, каждой нажатой клавише соответствует символ «●» (точка).

5. При вводе пароля следует помнить, что строчные и прописные буквы различаются. Допущенные ошибки при вводе исправляются так же, как и при заполнении текстового поля.
6. Нажать кнопку «Enter».

После нажатия кнопки «Enter» в системе защиты сначала проверяется возможность входа пользователя с данным именем и доменом, после чего проверяется соответствие с именем пользователя номера аппаратного идентификатора, зарегистрированного в системе защиты, и правильность указанного пользователем пароля. В случае успеха проверки, пользователю разрешается вход в систему, иначе вход в систему пользователю запрещается.

Примечание. При вводе имени и пароля переключение языка ввода (русский/английский) производится нажатием комбинации клавиш, установленной при настройке свойств клавиатуры. Текущий язык отображается индикатором клавиатуры.

Во время первого входа на ПК после установки СЗИ ВИ в области уведомлений Windows будет появляться сообщение о том, что ПК защищен СЗИ ВИ Dallas Lock (рис. 10).

2.5.2 Развертывание СЗИ ВИ для VMware vSphere vCenter

2.5.2.1 Установка компонента «Центр управления СЗИ ВИ Dallas Lock»

Порядок установки компонента «Центр управления СЗИ ВИ Dallas Lock» указан в п. 2.5.1 «Установка компонента «Центр управления СЗИ ВИ Dallas Lock»».

2.5.2.2 Установка агента DL vCenter for Windows на сервер виртуализации

Внимание! Установка платформы виртуализации VMware vSphere всегда должна производиться по пути, который предлагается инсталлятором платформы по умолчанию. В случае выбора любого другого каталога для установки, при инсталляции СЗИ ВИ произойдет ошибка копирования файлов и система не будет установлена.

Для установки агента DL vCenter for Windows обязательно **выполнение ряда условий:**

1. Текущий пользователь должен иметь права администратора ОС.
2. Перед установкой агента DL vCenter for Windows необходимо убедиться, что все сервисы vCenter стартовали, работают и доступны. Данное условие должно быть выполнено для дальнейшего корректного функционирования vCenter (в частности возможности подключаться к web-консоли) после установки агента DL vCenter for Windows.

Примечание. Перед установкой рекомендуется создать снимок виртуальной машины (snapshot) vCenter или точку восстановления на компьютере с vCenter.

Агент DL vCenter for Windows можно установить следующими способами:

1. Локально.
2. Удаленно.
3. Удаленно (в процессе ввода в ДБ с помощью мастера (подробнее см. п. 2.6.1 «Развертывание СЗИ ВИ для VMware vSphere vCenter»).

Локальная установка агента DL vCenter for Windows:

1. Запустить установочный файл «DLVI.msi» и дождаться завершения настройки Windows СЗИ ВИ Dallas Lock.
2. После завершения настройки запустится окно установщика, с помощью которого в программе установки необходимо выполнять действия по подсказкам программы. На каждом шаге установки предоставляется возможность отмены установки с возвратом сделанных изменений. Для этого служит кнопка «Назад». Выполнение следующего шага установки выполняется с помощью кнопки «Далее».
3. Для продолжения установки нажать кнопку «Далее».
4. Ввести номер лицензии продукта. Код активации технической поддержки при желании можно будет ввести позже (см. п. 11.2 «Работа с логами»).
5. Выбрать компонент «VMware vCenter for Windows» (см. рис. 5), нажать кнопку «Далее».

6. Опционально поставить флаг и заполнить поля подключения к Серверу лицензий (подробнее об использовании Сервера лицензий см. в документе «Инструкция по использованию сервера лицензий» ПФНА.501410.001 И4). Для продолжения установки нажать кнопку «Далее».
7. Появится уведомляющее окно о том, что исходные данные для установки заданы. Для установки нажать кнопку «Далее».
8. Далее последует процесс установки. Если процесс прошел без ошибок, то для завершения установки требуется перезагрузка ПК. После нажатия кнопки «Перезагрузить» через 1 минуту произойдет автоматическая перезагрузка ПК.

Если требуется выполнить перезагрузку позже, необходимо нажать кнопку «Завершить».

Удаленная установка агента DL vCenter for Windows

Для удаленной установки агента DL vCenter for Windows необходимо:

1. Запустить Консоль (подробнее см. п. 3.1 «Консоль»).
2. Выбрать пункт «Установить агенты DL Windows» в дереве «Агенты Windows» в блоке «Удаленная установка» либо из контекстного меню, вызываемого щелчком правой кнопки мыши на сервере управления доступом (рис. 13).

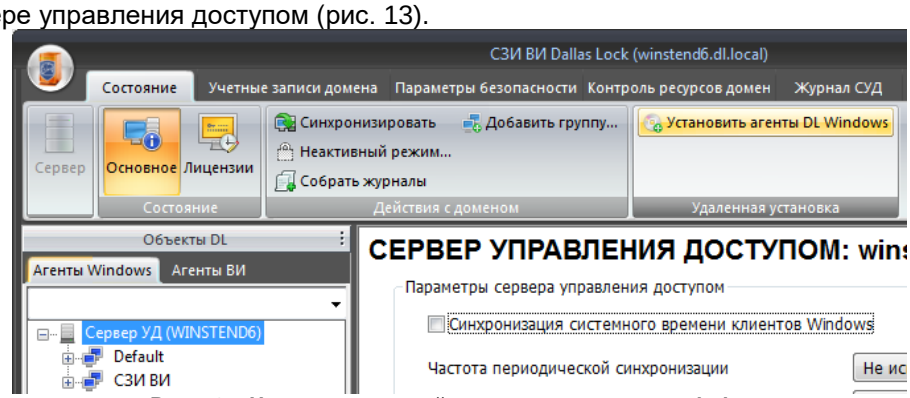


Рис. 13 – Начало удаленной установки агента DL Windows

3. В появившемся окне выбрать операцию «Добавить в список», обозначенную белым плюсом на зеленом фоне (рис. 14).

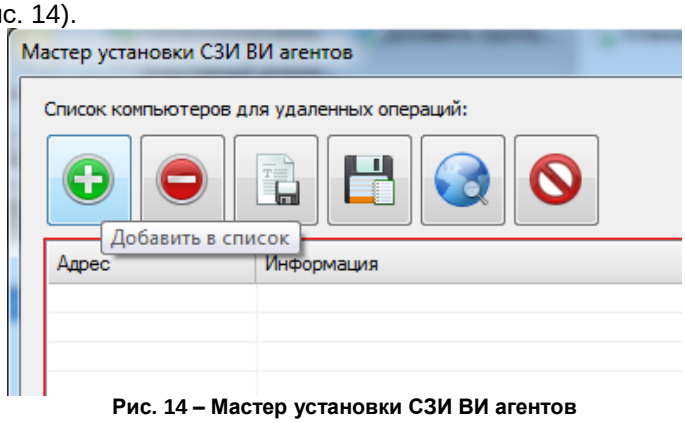


Рис. 14 – Мастер установки СЗИ ВИ агентов

4. В появившемся окне ввести имя или IP-адрес компьютера, на который необходимо установить агент DL vCenter for Windows (рис. 15). Для продолжения нажать кнопку «ОК».

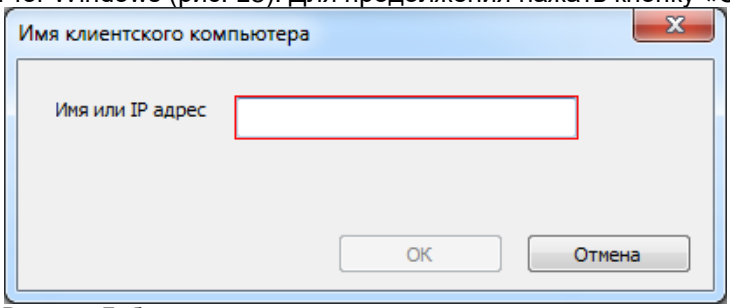


Рис. 15 – Добавление имени или IP-адреса клиентского компьютера

5. Левой кнопки мыши выбрать из списка компьютер, на который будет производиться установка агента и нажать кнопку «Продолжить».
6. Ввести данные администратора ОС компьютера, на который будет производиться установка агента (рис. 16):

- указать имя;
- указать домен;
- ввести пароль.

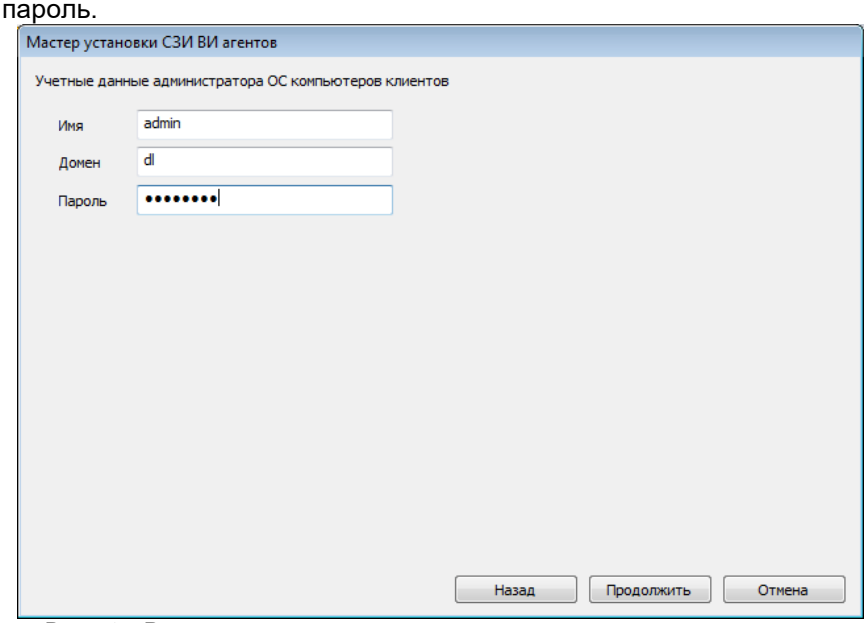


Рис. 16 – Ввод учетных данных администратора клиентского компьютера

Нажать кнопку «Продолжить».

7. Выбрать тип устанавливаемого агента «VMware vCenter for Windows» (рис. 17). Нажать кнопку «Продолжить».

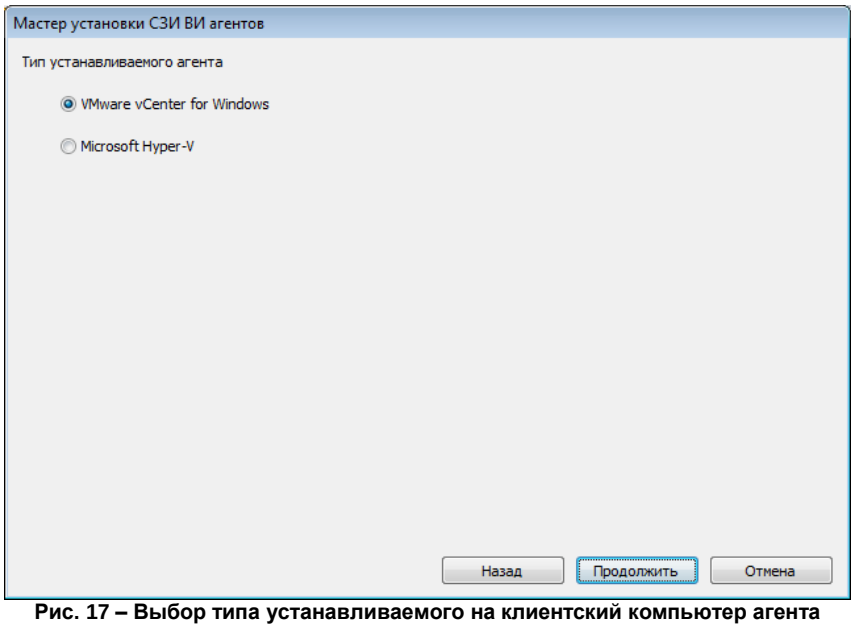


Рис. 17 – Выбор типа устанавливаемого на клиентский компьютер агента

8. Обязательно указать номер лицензии и путь к установочному файлу «DLVI.msi», с которого будет производиться установка агента (рис. 18). При необходимости заполнить остальные поля. Нажать кнопку «Продолжить».

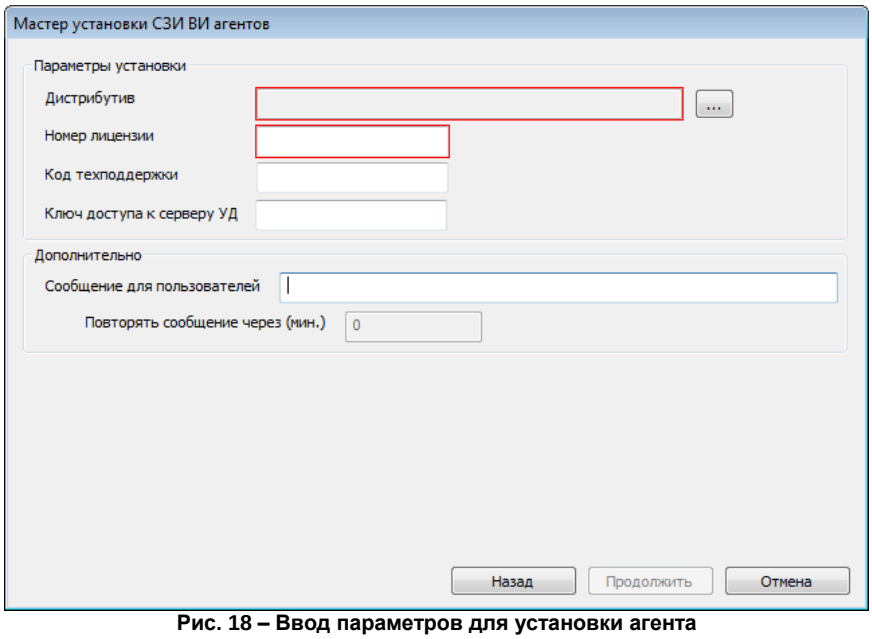


Рис. 18 – Ввод параметров для установки агента

При необходимости можно указать текст сообщения и периодичность его повтора для пользователей удаленного ПК.

9. Далее можно выбрать тип установки (без перезагрузки, с перезагрузкой, с последовательной установкой) и задать время, через которое должен будет перезагрузиться удаленный ПК (рис. 19). При выборе опции «Индивидуальная настройка интервалов» можно настроить время, через которое будет произведена перезагрузка для каждого ПК в отдельности.

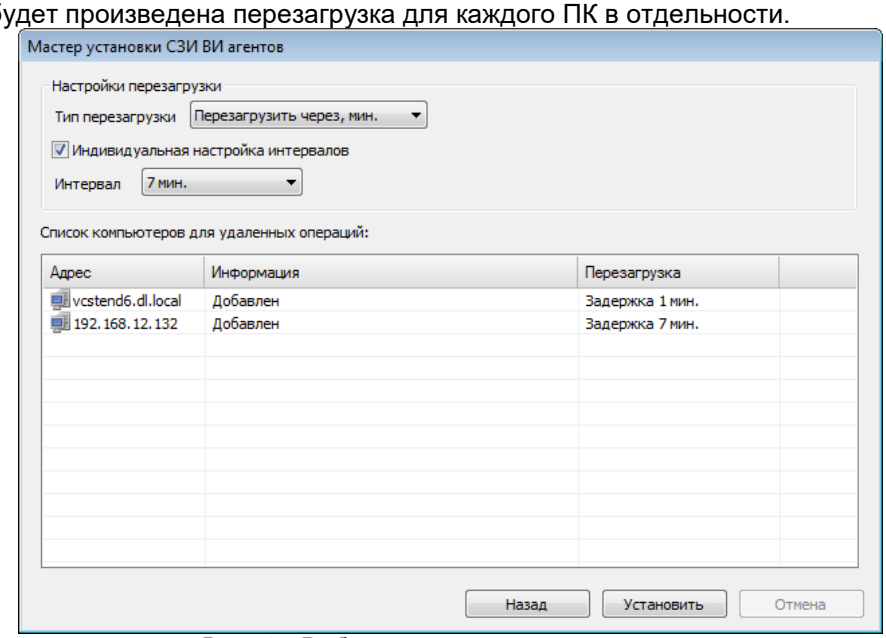


Рис. 19 – Выбор типа перезагрузки на клиенте

В случае выбора перезагрузки или последовательной установки с перезагрузкой на клиенте появится уведомление о том, что будет совершена перезагрузка (рис. 20).

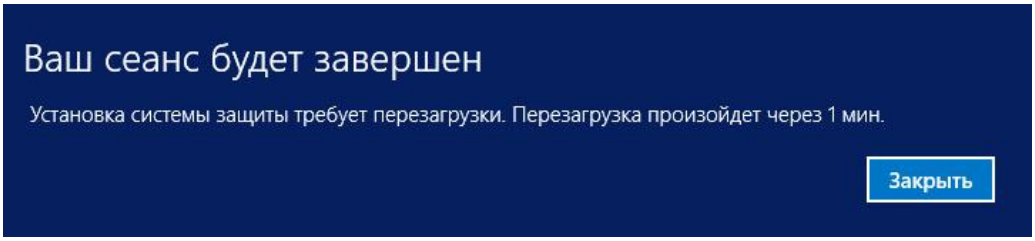


Рис. 20 – Уведомление о перезагрузке на клиенте

10. Далее мастер установки СЗИ ВИ агентов отобразит процесс подключения к удаленному компьютеру. В области уведомлений Windows появится сообщение об успешной установке агента DL (рис. 21). Для завершения процедуры необходимо нажать кнопку «Завершить» в окне мастера установки СЗИ ВИ агентов (рис. 22).

Рис. 21 – Сообщение об установке агента DL Windows

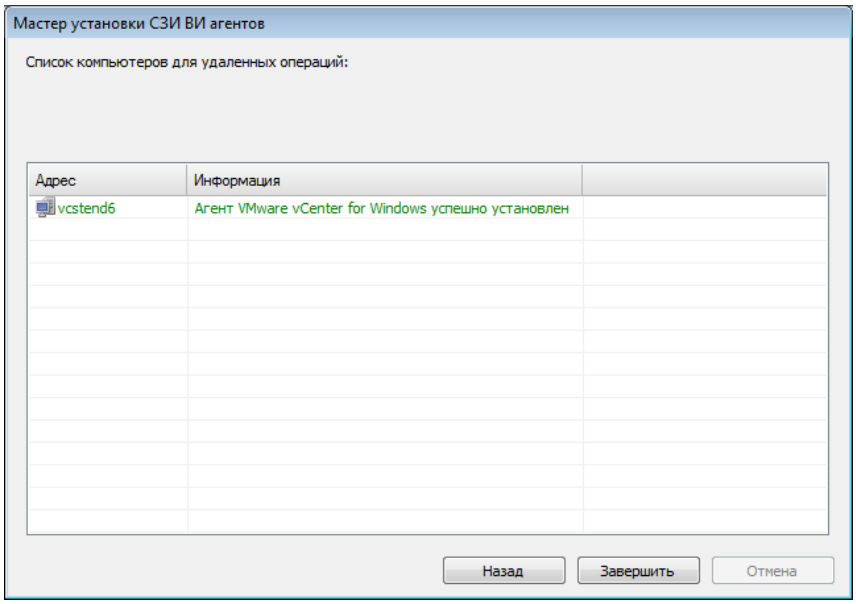


Рис. 22 – Завершение установки СЗИ ВИ агента

11. Если был выбран тип установки «без перезагрузки» или в выпадающем меню выбора интервала времени выбрано значение «Не перезагружать», то необходимо перезагрузить компьютер, на который был установлен агент DL.

2.5.2.3 Ввод в домен безопасности сервера виртуализации VMware vSphere vCenter for Windows

Для ввода сервера виртуализации vCenter for Windows в домен безопасности должен быть соблюден ряд условий:

1. Должен быть работающий ЦУ СЗИ ВИ.
2. Должны быть открыты TCP-порты, используемые ЦУ СЗИ ВИ для обмена данными с объектами ВИ и клиентами Windows (80, 443, 514, 7080, 8080, 8089, 17491, 17492, 17493).
3. Должна правильно выполняться операция преобразования имени компьютера в его IP-адрес.
4. Должна правильно выполняться операция обратного преобразования IP-адреса компьютера в его имя.

Для ввода сервера виртуализации vCenter for Windows в домен безопасности с помощью Консоли необходимо:

1. Открыть дерево «Агенты ВИ».
2. Выбрать уровень «vSphere» и открыть вкладку «Состояние».
3. В блоке «Действия с vSphere» нажать кнопку «Добавить сервер виртуализации vSphere…» либо выбрать данный пункт из контекстного меню на уровне vSphere (рис. 23).

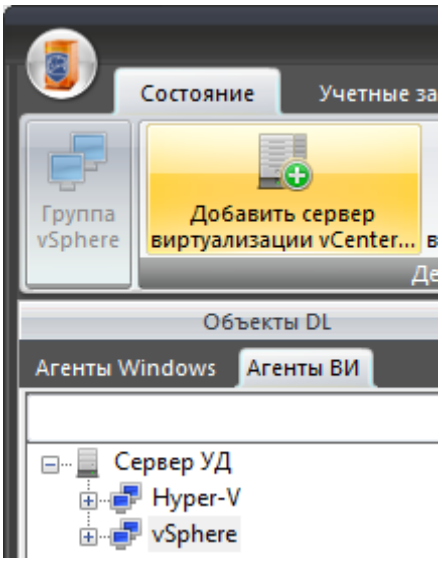


Рис. 23 – Добавление сервера виртуализации

4. В появившемся окне требуется ввести (рис. 24):
   - полное DNS-имя или IP-адрес сервера виртуализации;
   - данные учетной записи СЗИ ВИ клиента;
   - учетные данные сервера виртуализации.
5. При наличии внешнего PSC[8]:
   - установить флаг в поле «Внешний Platform Services Controller»;
   - выбрать тип ОС, установленной на сервере PSC (Windows/Linux);
   - ввести адрес PSC – полное DNS-имя сервера PSC;
   - ввести данные учетной записи администратора сервера PSC.

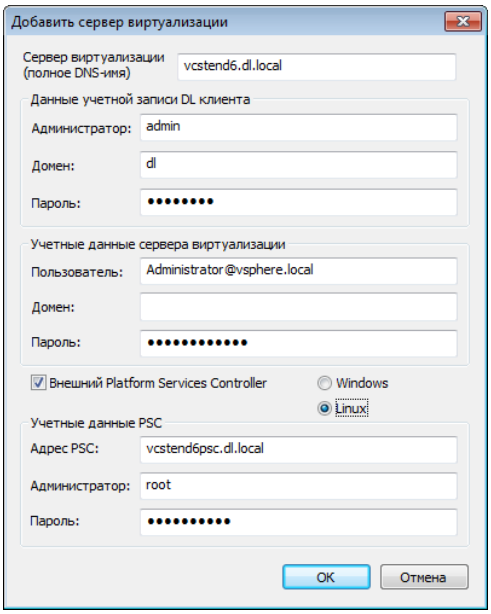


Рис. 24 – Ввод данных для добавления СВ

6. Нажать кнопку «ОК».

Если операция завершилась успешно, то в дереве «Агенты ВИ» появятся значки новых объектов ВИ.

2.5.2.4 Установка и удаление агента DL ESXi на гипервизоре ESXi

Внимание! В VMware ESXi 6.7 по умолчанию включен режим Secure Boot. Перед установкой агента DL vCSA на гипервизор данный режим необходимо отключить в настройках виртуальной машины.

[8] Действие доступно только для редакции «Расширенная».

Внимание! Установка агента DL ESXi не допускается на гипервизор ESXi с папкой scratch, находящейся на RAM диске (/tmp/scratch).

Примечание. Включение режима Lockdown Mode на гипервизоре существенно повышает уровень безопасности ВИ.

Подготовка к установке:

Внимание! Перед установкой агента DL ESXi рекомендуется выполнить настройку кластеров и их состава. В противном случае, после ввода (вывода) гипервизора в (из) состав(а) кластера или папки, необходимо снова установить учетные данные гипервизора. Далее, либо переустановить агента DL ESXi, либо перезагрузить его командой "/etc/init.d/confident-agentd restart" и выполнить настройку гипервизора в Консоли.

Внимание! Перед установкой агента DL ESXi необходимо убедиться, что на гипервизоре ESXi есть сконфигурированный VMFS раздел (Datastore).

Чтобы установить агент DL ESXi на гипервизор, необходимо указать учетные данные администратора гипервизора. Для этого требуется:

1. Открыть дерево «Агенты ВИ».
2. Выбрать уровень гипервизора и открыть категорию «Состояние» → «Основное».
3. Нажать кнопку «Установить учетные данные».
4. В появившемся окне ввести учетные данные гипервизора (рис. 25).

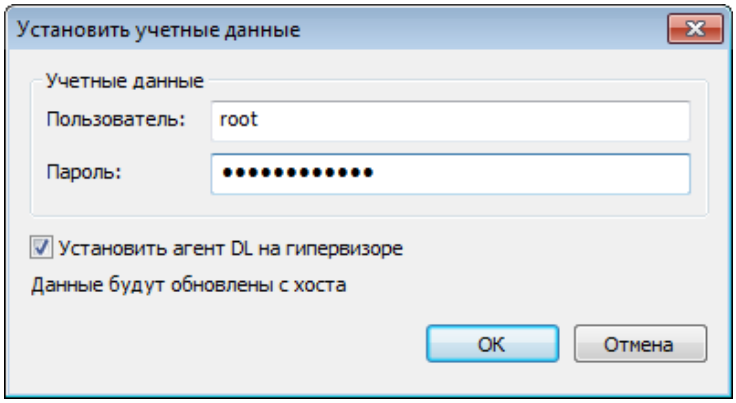


Рис. 25 – Установка учетных данных гипервизора

5. Чтобы автоматически установить агент DL после сохранения учетных данных гипервизора необходимо установить флаг «Установить агент DL на гипервизоре».
6. Нажать кнопку «ОК».

В случае если учетные данные уже установлены (об этом свидетельствует надпись «Учетные данные установлены»), то необходимо нажать кнопку «Установить агент на гипервизоре».

Статус учетных данных и агента DL ESXi отображаются на рабочей области (рис. 26).

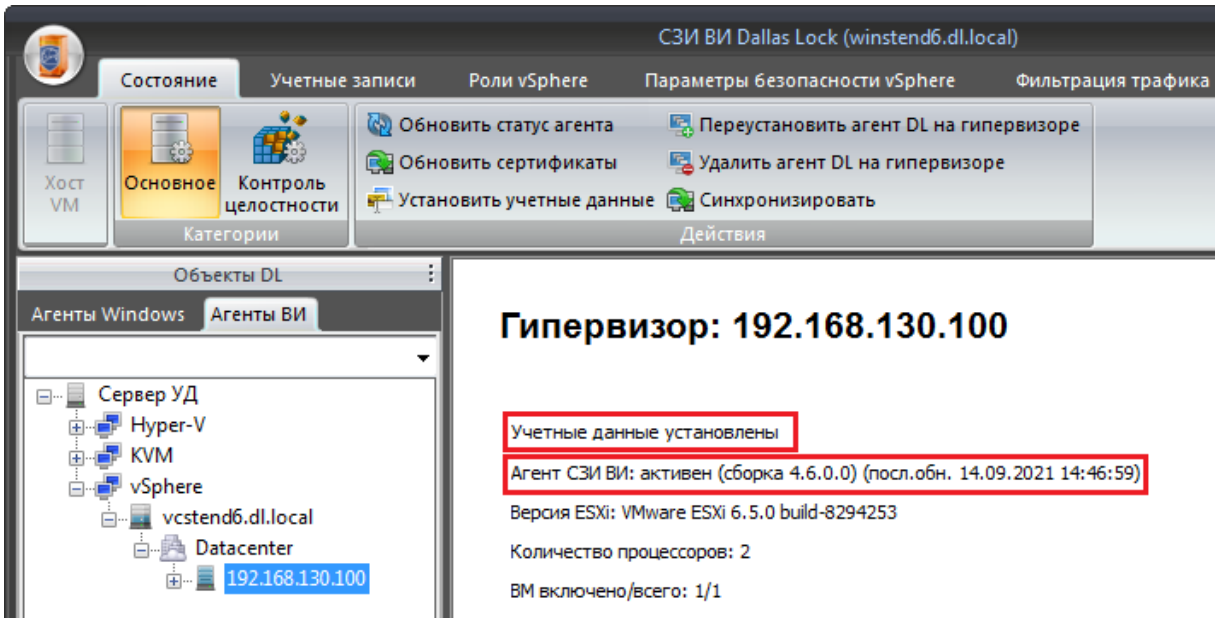


Рис. 26 – Статус учетных данных и агента DL

Для удаления агента DL ESXi, необходимо в категории действия нажать кнопку «Удалить агент DL на гипервизоре», либо вызвать щелчком правой кнопки мыши на гипервизоре контекстное меню и выбрать соответствующий пункт.

Примечание. В случае необходимости возможно удалить агент DL ESXi локально вручную. Для этого следует в командной строке выполнить команду "esxcli software vib remove -n confident-agentd".

2.5.3 Развертывание СЗИ ВИ для VMware vSphere vCSA

2.5.3.1 Установка компонента «Центр управления СЗИ ВИ Dallas Lock»

Порядок установки компонента «Центр управления СЗИ ВИ Dallas Lock» указан в п. 2.5.1 «Установка компонента «Центр управления СЗИ ВИ Dallas Lock»».

2.5.3.2 Установка агента DL vCSA и ввод в домен безопасности сервера виртуализации vCSA

Внимание! Перед установкой агента DL vCSA в инфраструктуру vSphere 7.0.3 необходимо на СВ vCSA в файле "/etc/vmware-rhttpproxy/endpoints.conf.d/vpxd-rhttpproxy-endpoint.conf" добавить следующую строку в начало файла - “/sdk local 8085 redirect allow”.
Далее необходимо перезапустить службу rhttpproxy выполнив следующую команду – “systemctl restart rhttpproxy”.

Внимание! Перед установкой агента DL vCSA необходимо проверить срок действия пароля root на СВ. При истекшем сроке действия пароля root для vCSA установка агента DL vCSA не будет осуществлена.

Внимание! Перед установкой агента DL vCSA необходимо проверить корректность установленной даты и времени на СВ. При расхождении даты и времени на vCSA с ЦУ СЗИ ВИ установка агента DL vCSA не будет осуществлена.

Внимание! Перед установкой агента DL vCSA необходимо убедиться, что настроен автостарт ВМ с установленным на ней СВ.

Примечание. При работе с vCSA необходимо заблокировать доступ по SSH к vCSA (см. п. 5.3.1.1 «Параметры входа для vSphere»), и удалить привилегии доступа локальным пользователям vCSA.

Для установки агента DL vCSA и ввода сервера виртуализации vCSA в домен безопасности с помощью Консоли необходимо:

1. Открыть дерево «Агенты ВИ».
2. Выбрать уровень «vSphere» и открыть вкладку «Состояние».
3. В блоке «Действия с vSphere» нажать кнопку «Добавить сервер виртуализации vCSA…» либо выбрать данный пункт из контекстного меню на уровне vSphere.
4. В появившемся окне требуется ввести (рис. 27):
   - полное DNS-имя или IP-адрес сервера виртуализации;
   - данные учетной записи СЗИ ВИ клиента;
   - учетные данные сервера виртуализации.

Внимание! В случае, если IP-адрес сервера виртуализации vCSA является динамическим, его DNS-имя не должно содержать кириллические символы.

5. При наличии внешнего PSC[9]:
   - установить флаг в поле «Внешний Platform Services Controller»;
   - выбрать тип ОС, установленной на сервере PSC (Windows/Linux);
   - ввести адрес PSC – полное DNS-имя сервера PSC;
   - ввести данные учетной записи администратора сервера PSC.
6. Выбрать способ установки агента:
   - VMware API – в случае, если VCSA развернут как виртуальная машина на гипервизоре (т.н. вложенная виртуализация);
   - SSH + SFTP – в случае, если VCSA развернут на локальной машине.

Примечание. В случае ошибки установки агента vcsa попробуйте переключить способ установки агента на другой.

Примечание. Метод установки «VMware API» не работает, если хост ESXi, на котором развернута ВМ с vCSA, не введен в vCSA.

[9] Действие доступно только для редакции «Расширенная».

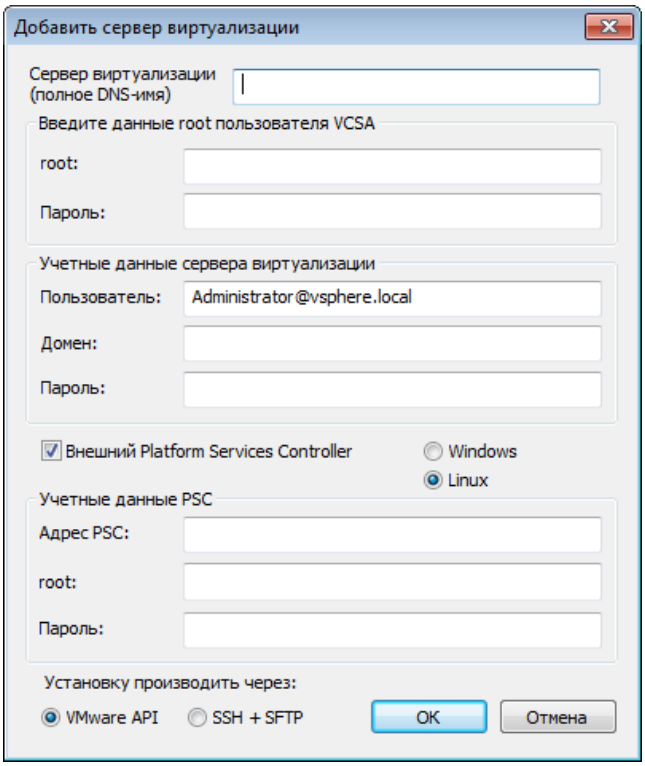


Рис. 27 – Установка агента DL vCSA и ввод в домен безопасности сервера виртуализации vCSA

7. Нажать кнопку «ОК».

Если операция завершилась успешно, то в дереве «Агенты ВИ» в ветке vSphere появятся значки новых объектов ВИ.

2.5.4 Развертывание СЗИ ВИ для Hyper-V

2.5.4.1 Установка компонента «Центр управления СЗИ ВИ Dallas Lock»

Порядок установки компонента «Центр управления СЗИ ВИ Dallas Lock» указан в п. 2.5.1 «Установка компонента «Центр управления СЗИ ВИ Dallas Lock»».

2.5.4.2 Установка агента DL Hyper-V

Агент DL Hyper-V можно установить двумя способами:

1. Локально.
2. Удаленно.
3. Удаленно (в процессе ввода в ДБ с помощью мастера (подробнее см. п. 2.6.3 «Развертывание СЗИ ВИ для Hyper-V»).

Локальная установка агента DL Hyper-V

Примечание. Перед локальной установкой агента DL Hyper-V на компьютер с ОС Windows Server 2012, 2012 R2, 2016, 2019 или 2022, установленной в режиме «Server Core», необходимо убедиться, что в ОС запущен хотя бы один экземпляр консоли.

Интерфейс установки агента DL Hyper-V полностью идентичен интерфейсу установки Центра управления СЗИ ВИ Dallas Lock на шагах установки с первого по четвертый (п. 2.5.1 «Установка компонента «Центр управления СЗИ ВИ Dallas Lock»»).

1. Запустить установочный файл «DLVI.msi» и дождаться завершения копирования файлов. Агент DL Hyper-V всегда по умолчанию устанавливается в папку «C:\DLVI».

2. После завершения настройки запустится окно установщика, с помощью которого в программе установки необходимо выполнять действия по подсказкам программы. На каждом шаге установки предоставляется возможность отмены установки с возвратом сделанных изменений. Для этого служит кнопка «Назад». Выполнение следующего шага установки выполняется с помощью кнопки «Далее».

Для продолжения установки нажать кнопку «Далее».

3. Ввести номер лицензии продукта. Код активации технической поддержки при желании можно будет ввести позже (см. п.11.3 «Настройки лицензирования»).

4. Выбрать компонент «Microsoft Hyper-V/SC VMM» (рис. 28), нажать кнопку «Установить».

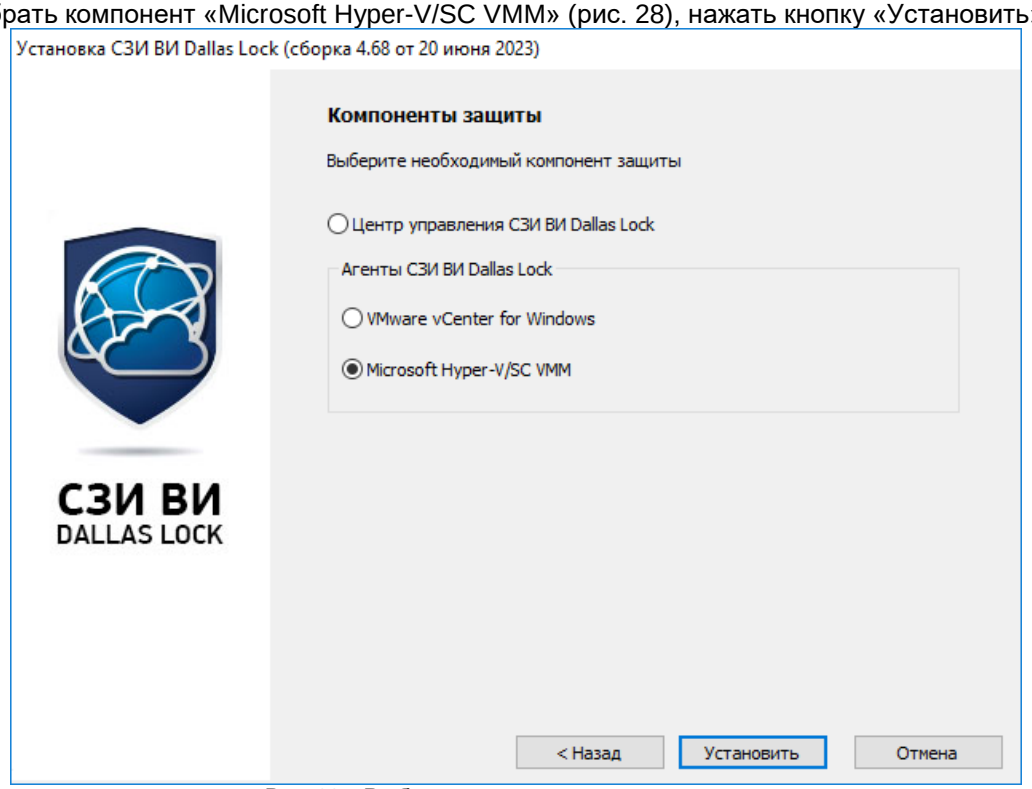


Рис. 28 – Выбор типа устанавливаемого агента

5. Последует процесс установки (рис. 29). Если процесс прошел без ошибок, то для завершения установки требуется перезагрузка ПК. После нажатия кнопки «Перезагрузить» через 1 минуту произойдет автоматическая перезагрузка ПК. Если требуется выполнить перезагрузку позже, необходимо нажать кнопку «Завершить».

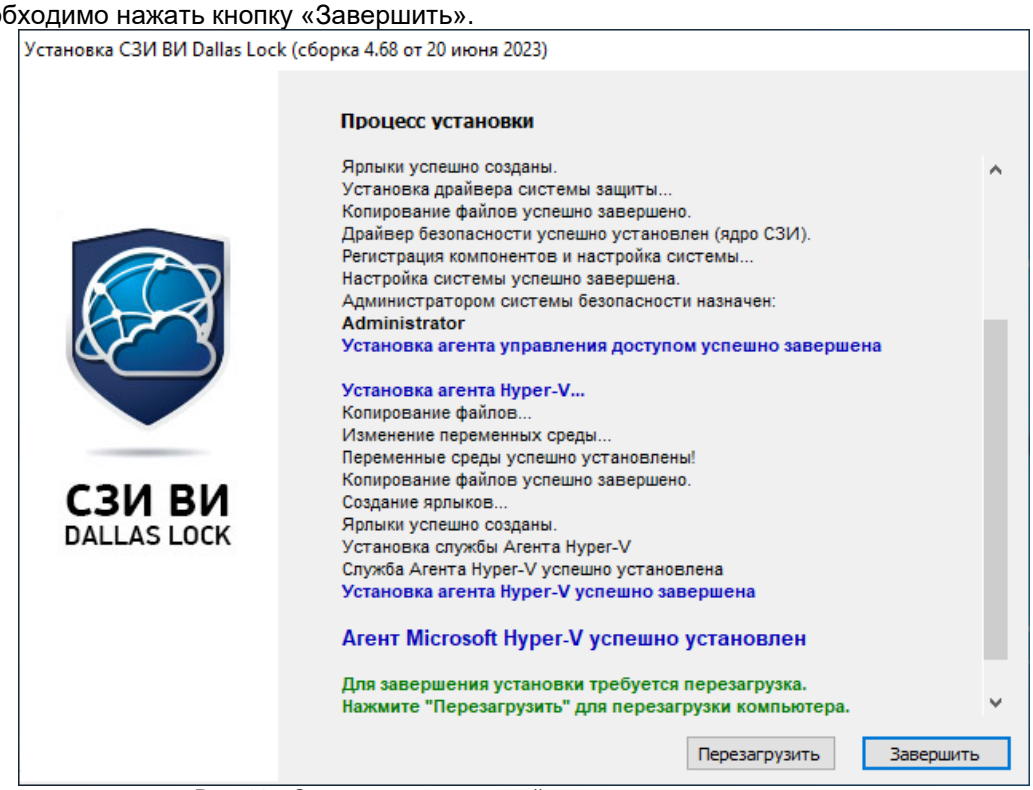


Рис. 29 – Завершение локальной установки агента DL Hyper-V

Удаленная установка агента DL Hyper-V

Порядок удаленной установки агента DL Hyper-V аналогичен порядку удаленной установки агента DL vCenter for Windows.
Для удаленной установки агента DL Hyper-V необходимо:

1. Запустить Консоль (подробнее см. п. 3.1 «Консоль»).

2. В дереве «Агенты Windows» в категории «Удаленная установка» выбрать пункт «Установить агенты DL Windows» (см. рис. 13).
3. В появившемся окне выбрать операцию «Добавить в список», обозначенную белым плюсом на зеленом фоне (см. рис. 14).
4. В появившемся окне ввести полное DNS-имя или IP-адрес компьютера, на который необходимо установить агент DL Hyper-V. Для продолжения нажать кнопку «ОК» (см. рис. 15).
5. Левой кнопки мыши выбрать из списка компьютер, на который будет производиться установка агента и нажать кнопку «Продолжить».
6. Ввести данные администратора ОС компьютера, на который будет производиться установка агента (см. рис. 16):
   - указать имя;
   - указать домен;
   - ввести пароль.

   Нажать кнопку «Продолжить».
7. Выбрать тип устанавливаемого агента «Microsoft Hyper-V» (рис. 30). Нажать кнопку «Продолжить».

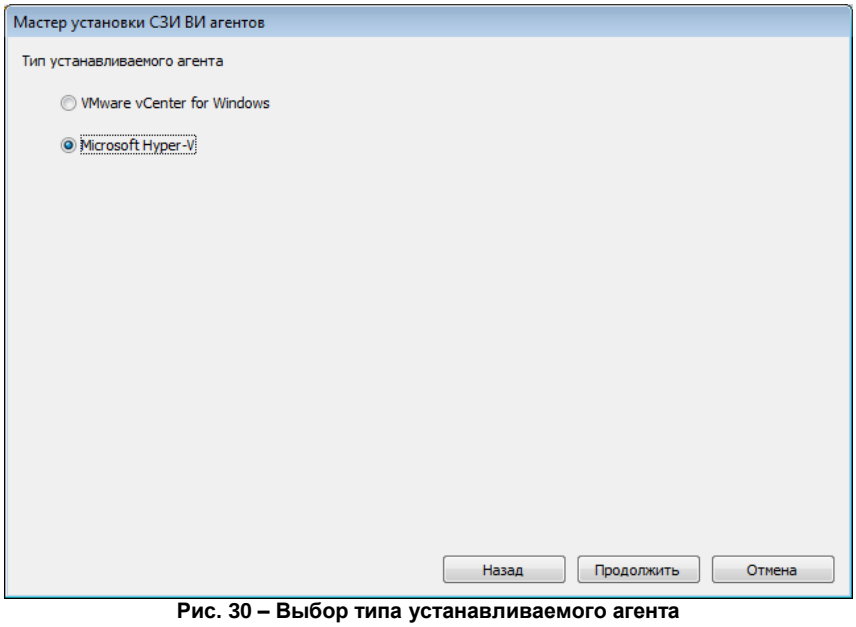


Рис. 30 – Выбор типа устанавливаемого агента

8. Обязательно указать номер лицензии и путь к установочному файлу «DLVI.msi», с которого будет производиться установка агента. При необходимости заполнить остальные поля (см. рис. 18). Нажать кнопку «Продолжить».
9. Выбрать тип установки (без перезагрузки, с перезагрузкой, последовательная установка) и задать интервал (см. рис. 19). Нажать кнопку «Продолжить».
10. Далее мастер установки СЗИ ВИ агентов отобразит процесс подключения к удаленному компьютеру. Для завершения процедуры необходимо нажать кнопку «Завершить».
11. Если был выбран тип установки «без перезагрузки» или в выпадающем меню выбора интервала времени выбрано значение «Не перезагружать», то необходимо перезагрузить компьютер, на который был установлен агент DL.

2.5.4.3 Ввод в домен безопасности сервера виртуализации Hyper-V

1. Открыть дерево «Агенты ВИ» в Консоли.
2. Выбрать уровень гипервизора «Hyper-V» и открыть вкладку «Состояние».
3. В блоке «Действия с Hyper-V» или через контекстное меню нажать кнопку «Добавить сервер виртуализации Hyper-V» (рис. 31).

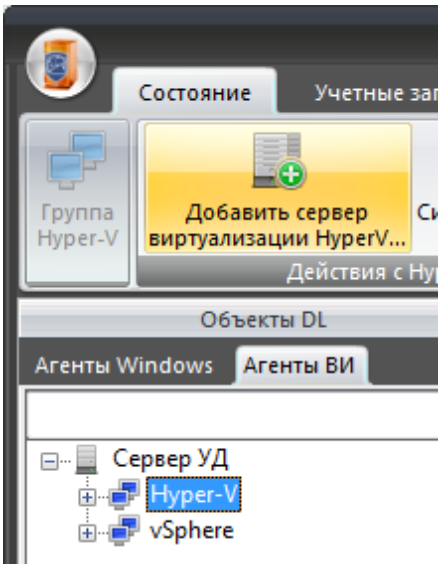


Рис. 31 – Добавление СВ Hyper-V

4. В появившемся окне прописать полное DNS-имя сервера виртуализации, ввести данные администратора (рис. 32).
5. В случае, если сервер виртуализации Hyper-V имеет кластерную роль и в СЗИ ВИ требуется работа с ним, как с кластером, нужно поставить флаг в поле «СВ Hyper-V» имеет кластерную роль.

Примечание. Перед добавлением СВ с кластерной ролью необходимо включить сессии-исключения на всех узлах кластера с обязательно последующей перезагрузкой узлов.

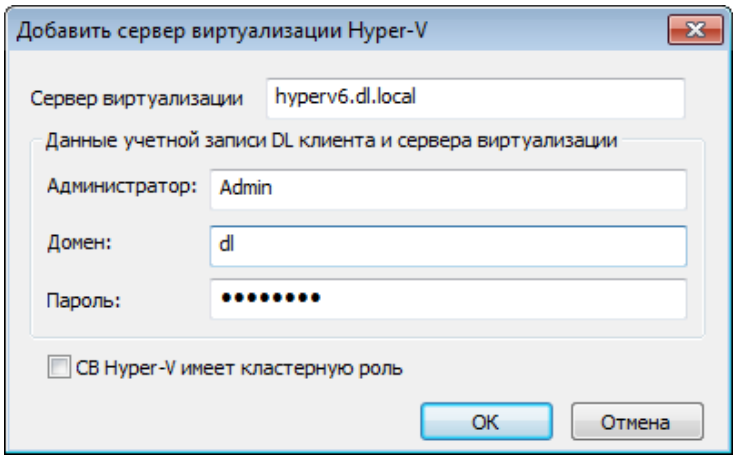


Рис. 32 – Ввод учетных данных СВ Hyper-V

6. Нажать кнопку «ОК».

Запустится процесс подключения к серверу виртуализации и после успешного выполнения процедуры в дереве ВИ в поддереве Hyper-V появится объект нового СВ. Также соответствующий windows-клиент появится в дереве Агентом Windows в группе «СЗИ ВИ».

В случае, если СВ Hyper-V добавлялся с кластерной ролью, в дереве ВИ в поддереве Hyper-V будет создан специальный объект Кластера Hyper-V с соответствующим именем. Объект нового СВ Hyper-V с кластерной ролью в свою очередь будет добавлен в поддерево объекта Кластера.

Внимание! СЗИ ВИ «Dallas Lock» поддерживает управление серверами Hyper-V через System Center Virtual Machine Manager и Failover Cluster Manager, при этом следует учитывать, что в режиме использования данных инструментов управления кластеризацией типовые операции могут отличаться от выполняемых операций, вызванных через Консоль ЦУ СЗИ ВИ.

2.5.5 Развертывание СЗИ ВИ для KVM

2.5.5.1 Установка компонента «Центр управления СЗИ ВИ Dallas Lock»

Порядок установки компонента «Центр управления СЗИ ВИ Dallas Lock» указан в п. 2.5.1 «Установка компонента «Центр управления СЗИ ВИ Dallas Lock»».

2.5.5.2 Установка и удаление агента DL KVM и ввод в домен безопасности сервера виртуализации KVM

Перед установкой агента DL KVM, необходимо убедиться, что к гипервизору открыт доступ по SSH и отключена политика «Вход: блокировать протокол SSH» (подробнее см. п. 5.3.1.3 «Параметры входа для KVM/oVirt/zVirt/HOSTVM»). Далее необходимо указать учетные данные администратора гипервизора. Для этого требуется:

1. Открыть дерево «Агенты ВИ».
2. Выбрать уровень «KVM» и открыть вкладку «Состояние».
3. Нажать кнопку «Добавить сервер виртуализации KVM…», либо выбрать данный пункт из контекстного меню на уровне «KVM» (рис. 33).

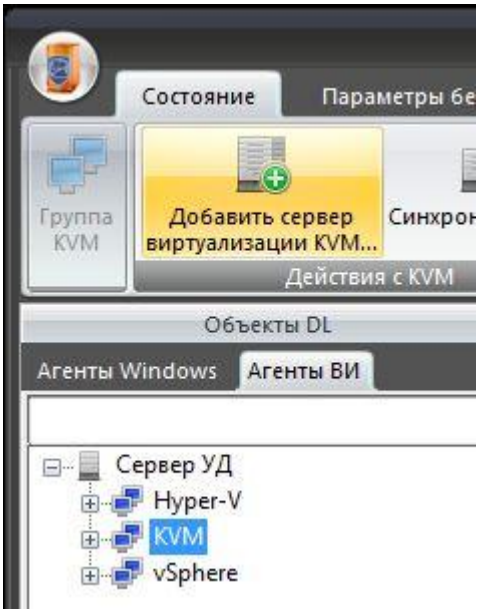


Рис. 33 – Добавление сервера виртуализации

4. В появившемся окне требуется ввести (рис. 34):
   - полное DNS-имя в сети или IP-адрес сервера виртуализации;
   - данные учетной записи пользователя.

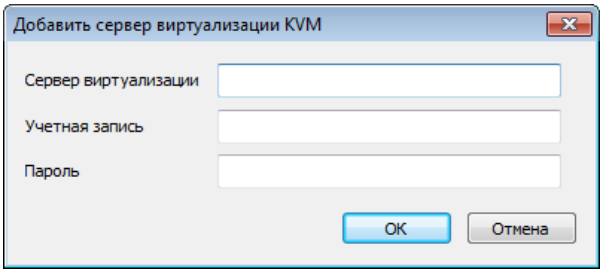


Рис. 34 – Ввод данных для добавления СВ

5. Нажать кнопку «ОК».

Если операция завершилась успешно, то в дереве «Агенты ВИ» появятся значки новых объектов ВИ.

Для удаления гипервизора из домена безопасности и агента DL KVM необходимо в категории действия нажать кнопку «Удалить из ВИ».

2.5.6 Развертывание СЗИ ВИ для oVirt/zVirt/HOSTVM/РЕД Вирт

2.5.6.1 Установка компонента «Центр управления СЗИ ВИ Dallas Lock»

Порядок установки компонента «Центр управления СЗИ ВИ Dallas Lock» указан в п. 2.5.1 «Установка компонента «Центр управления СЗИ ВИ Dallas Lock»».

2.5.6.2 Установка и удаление агента DL Engine и ввод в домен безопасности сервера виртуализации oVirt/zVirt/HOSTVM/РЕД Вирт

Перед установкой агента DL Engine, необходимо убедиться, что к СВ открыт доступ по SSH и отключена политика «Вход: блокировать протокол SSH» (подробнее см. п. 5.3.1.3 «Параметры входа для KVM/oVirt/zVirt/HOSTVM»). Далее для ввода в домен безопасности и установки агента DL Engine необходимо:

1. Открыть дерево «Агенты ВИ».
2. Выбрать уровень «KVM» и открыть вкладку «Состояние».
3. Нажать кнопку «Добавить сервер виртуализации KVM…», либо выбрать данный пункт из контекстного меню на уровне «KVM» (рис. 35).

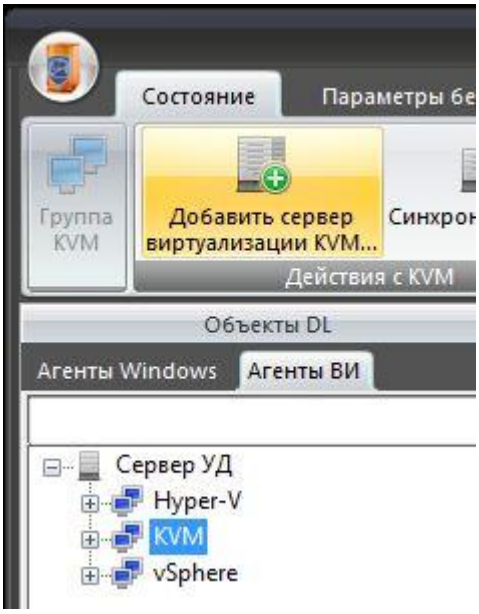


Рис. 35 – Добавление сервера виртуализации

4. В появившемся окне требуется (рис. 36):
   - ввести полное DNS-имя в сети или IP-адрес сервера виртуализации;
   - ввести данные учетной записи пользователя KVM (администратора ОС);
   - установить флаг в поле «Виртуальная инфраструктура oVirt»;
   - ввести данные учетной записи пользователя oVirt/zVirt/HOSTVM/РЕД Вирт.

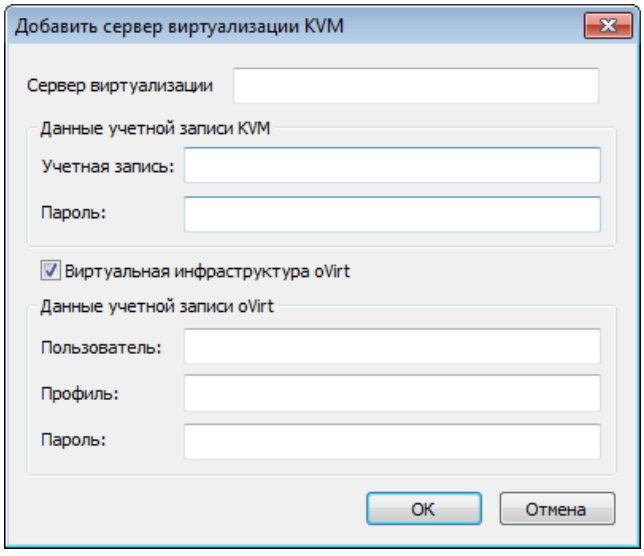


Рис. 36 – Ввод данных для добавления СВ

5. Нажать кнопку «ОК».

Если операция завершилась успешно, то в дереве «Агенты ВИ» появятся значки новых объектов ВИ.

Для удаления СВ из домена безопасности и агента DL Engine необходимо в категории действия нажать кнопку «Удалить из ВИ».

Примечание. В случае необходимости возможно удалить агент DL Engine локально вручную. Для этого следует в командной строке выполнить команду "/opt/confident/bin/uninstall_agent.sh".

2.5.6.3 Установка и удаление агента DL Host на гипервизоре oVirt/zVirt/HOSTVM/РЕД Вирт

Чтобы установить агент DL Host на гипервизор, необходимо указать учетные данные администратора гипервизора. Для этого требуется:

1. Открыть дерево «Агенты ВИ».
2. Выбрать уровень гипервизора и открыть категорию «Состояние» → «Основное».
3. Нажать кнопку «Установить учетные данные».
4. В появившемся окне ввести учетные данные гипервизора (рис. 37).

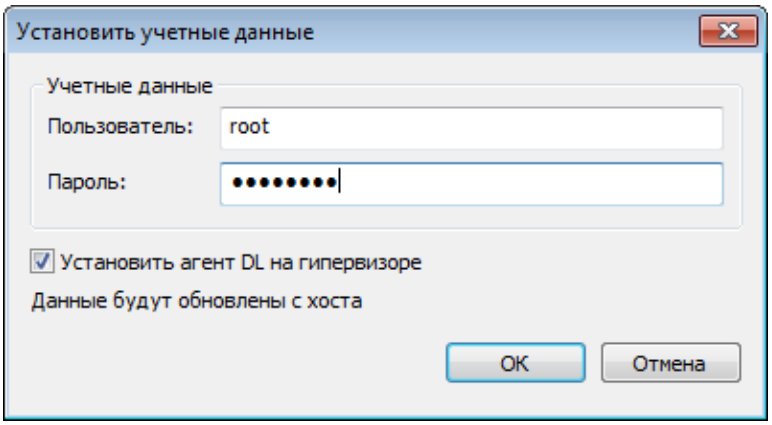


Рис. 37 – Установка учетных данных гипервизора

5. Чтобы автоматически установить агент DL после сохранения учетных данных гипервизора необходимо установить флаг «Установить агент DL на гипервизоре».
6. Нажать кнопку «ОК».

В случае если учетные данные уже установлены (об этом свидетельствует надпись «Учетные данные установлены»), то необходимо нажать кнопку «Установить агент на гипервизоре».

Статус учетных данных и агента DL Host отображаются на рабочей области (рис. 38).

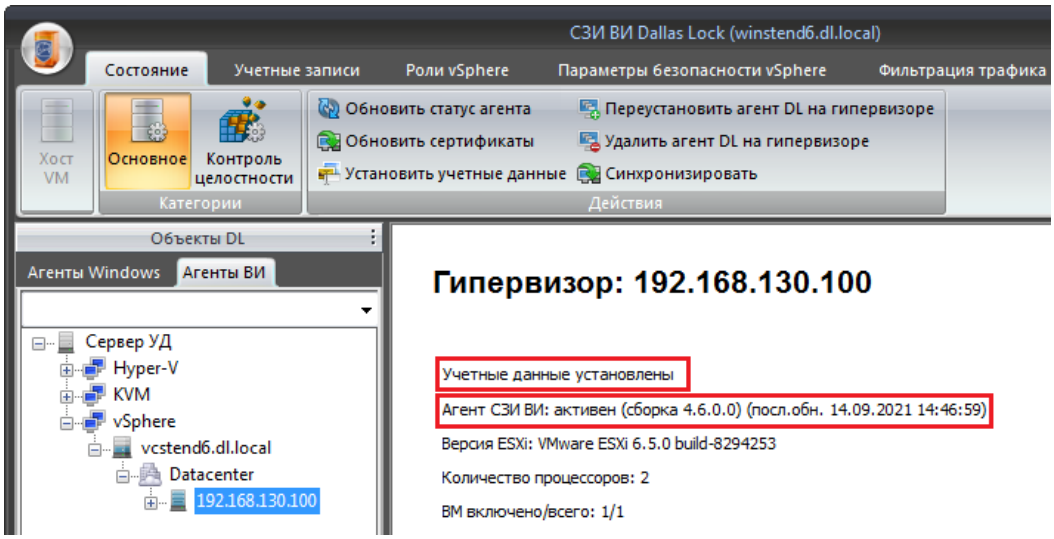


Рис. 38 – Статус учетных данных и агента DL

Для удаления агента DL Host, необходимо в категории действия нажать кнопку «Удалить агент DL на гипервизоре», либо вызвать щелчком правой кнопки мыши на гипервизоре контекстное меню и выбрать соответствующий пункт.

Примечание. В случае необходимости возможно удалить агент DL Host локально вручную. Для этого следует в командной строке выполнить команду "/opt/confident/bin/uninstall_agent.sh".

2.6 Развертывание компонентов СЗИ ВИ с помощью мастера

Данный способ развертывания объединяет установку компонентов защиты и ввод в домен безопасности. Также, благодаря разделению ввода данных на этапы, сокращается количество возможных ошибок со стороны администратора информационной безопасности.

2.6.1 Развертывание СЗИ ВИ для VMware vSphere vCenter

2.6.1.1 Установка компонента «Центр управления СЗИ ВИ Dallas Lock»

Порядок установки компонента «Центр управления СЗИ ВИ Dallas Lock» указан в п. 2.5.1 «Установка компонента «Центр управления СЗИ ВИ Dallas Lock»».

2.6.1.2 Ввод в домен безопасности и удаленная установка агента DL vCenter for Windows на сервер виртуализации с помощью мастера

Для ввода сервера виртуализации vCenter for Windows в домен безопасности должен быть соблюден ряд условий:

1. Должен быть работающий ЦУ СЗИ ВИ.
2. Должны быть открыты TCP-порты, используемые ЦУ СЗИ ВИ для обмена данными с объектами ВИ и клиентами Windows (80, 443, 514, 7080, 8080, 8089, 17491, 17492, 17493).
3. Должна правильно выполняться операция преобразования имени компьютера в его IP-адрес.
4. Должна правильно выполняться операция обратного преобразования IP-адреса компьютера в его имя.

Для ввода в домен безопасности и удаленной установки агента DL vCenter for Windows необходимо:

1. Запустить Консоль.
2. Во вкладке «Агенты ВИ» выбрать уровень «Сервер УД» и открыть вкладку «Состояние».
3. В блоке «Действия с ВИ» нажать кнопку «Добавить сервер виртуализации» (рис. 39).

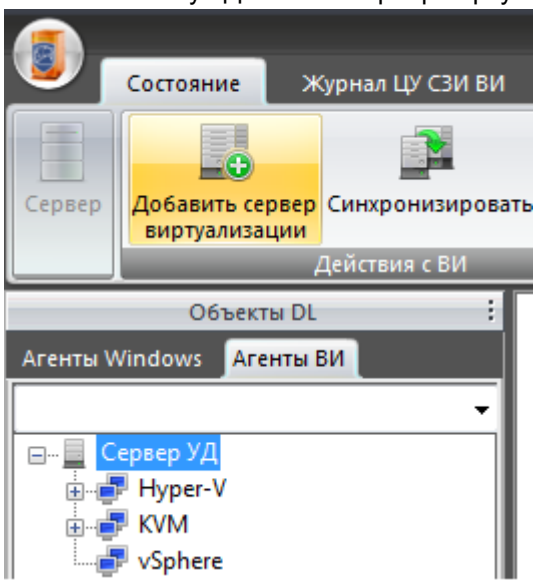


Рис. 39 – Добавление сервера виртуализации

4. В появившемся информационном окне, после ознакомления со справочной информацией необходимо нажать кнопку «Далее».
5. Ввести IP-адрес или полное доменное имя сервера виртуализации и нажать кнопку «Далее» (рис. 40).

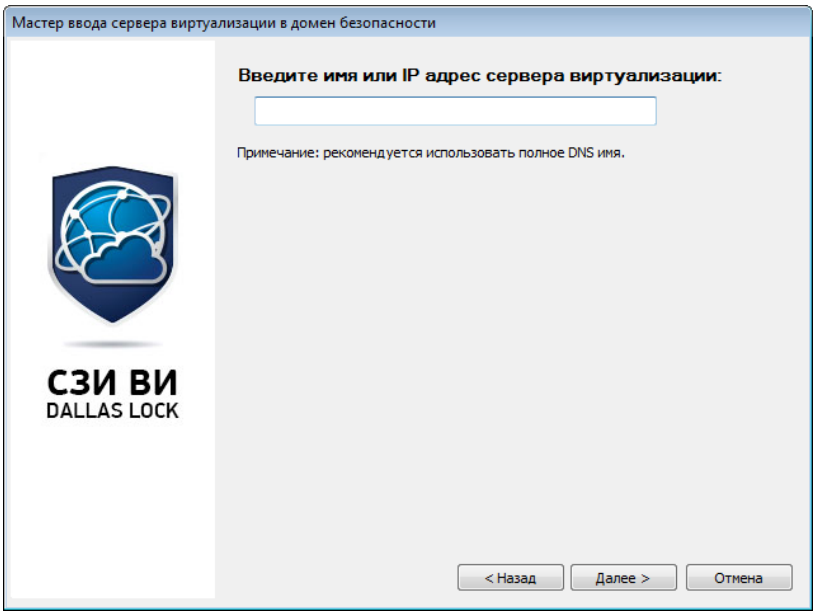


Рис. 40 – Ввод имени или IP-адреса сервера виртуализации

6. Выбрать тип агента VMware vCenter for Windows (рис. 41).

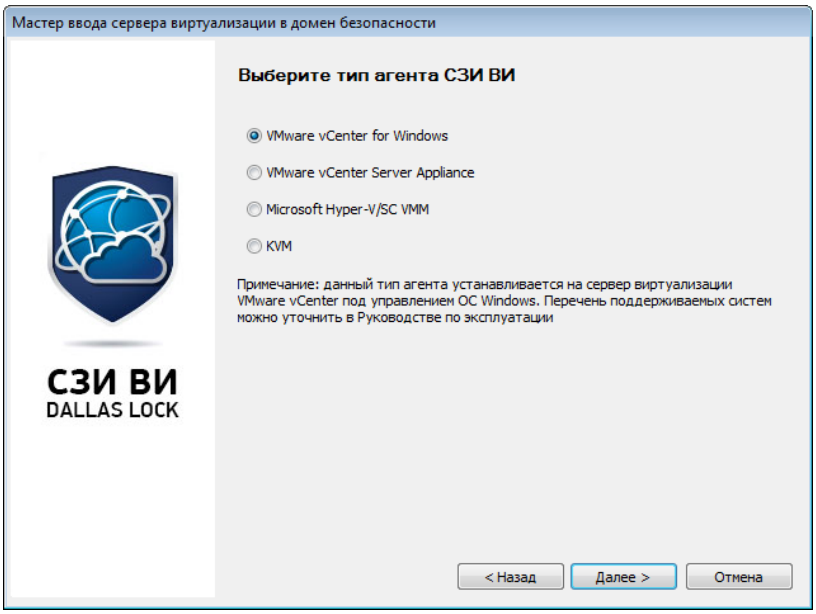


Рис. 41 – Выбор типа устанавливаемого агента

Нажать кнопку «Далее».

7. Ввести учетные данные администратора ОС (рис. 42):

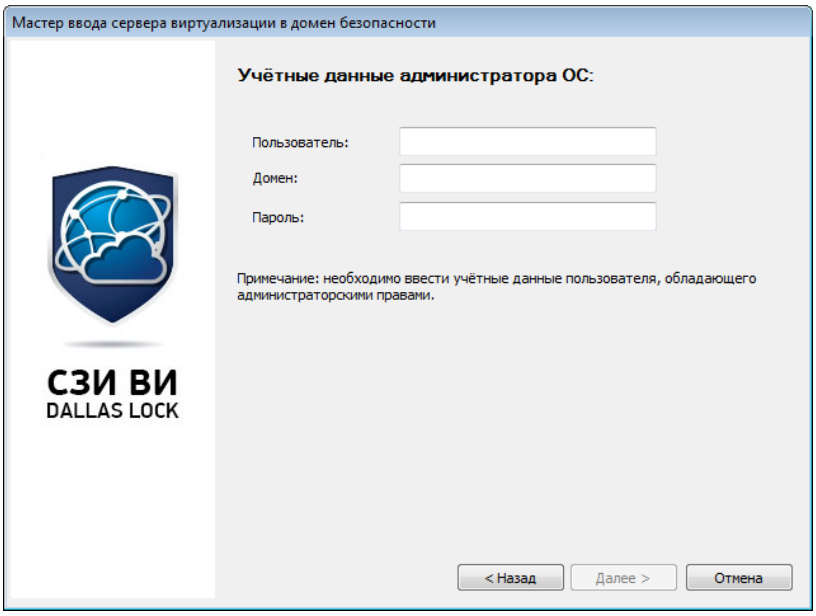


Рис. 42 – Ввод учетных данных администратора клиентского компьютера

Нажать кнопку «Далее».

8. Если требуется удаленная установка агента DL[10] на СВ необходимо установить флаг в поле «Установить компоненты защиты» (рис. 43).

В активировавшиеся поля ввести следующие данные:

- номер лицензии;
- код технической поддержки;
- ключ доступа к СУД (подробнее см п. 5.6 «Ключи удаленного доступа»).

Указать путь к дистрибутиву СЗИ ВИ.

Если требуется перезагрузить СВ после установки компонентов защиты и вывести сообщение для пользователей необходимо установить флаг в поле «Перезагрузить удаленный компьютер после установки» и заполнить необходимые поля.

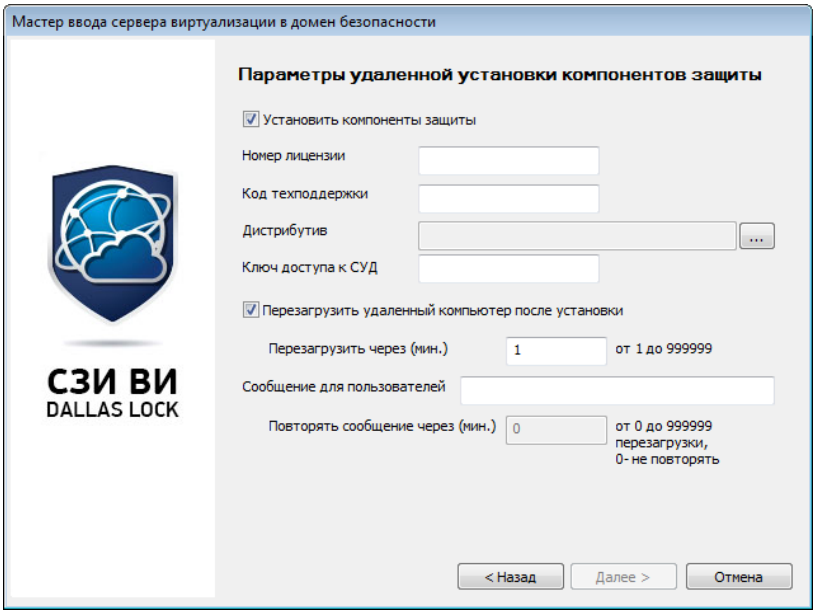


Рис. 43 – Ввод параметров для установки агента

Нажать кнопку «Далее».

9. Ввести учетные данные администратора vSphere (рис. 44)

[10] Без установленных компонентов защиты ввод в домен безопасности невозможен.

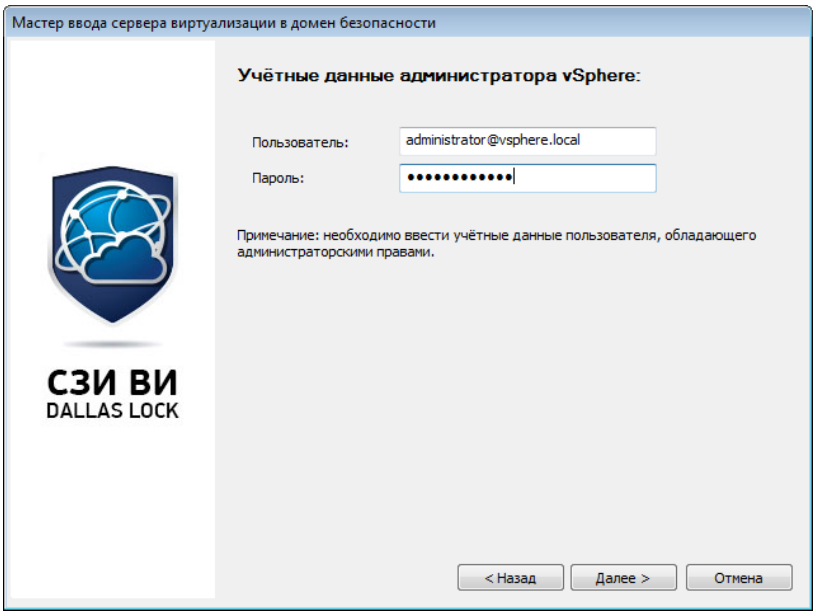


Рис. 44 – Ввод учетных данных первичного администратора vSphere

Нажать кнопку «Далее».

10. При наличии внешнего Platform Service Controller (PSC)[11].

1) Если требуется подключение к внешнему необходимо установить флаг в поле «Подключиться к внешнему PSC» и ввести IP-адрес или полное доменное имя сервера (рис. 45).

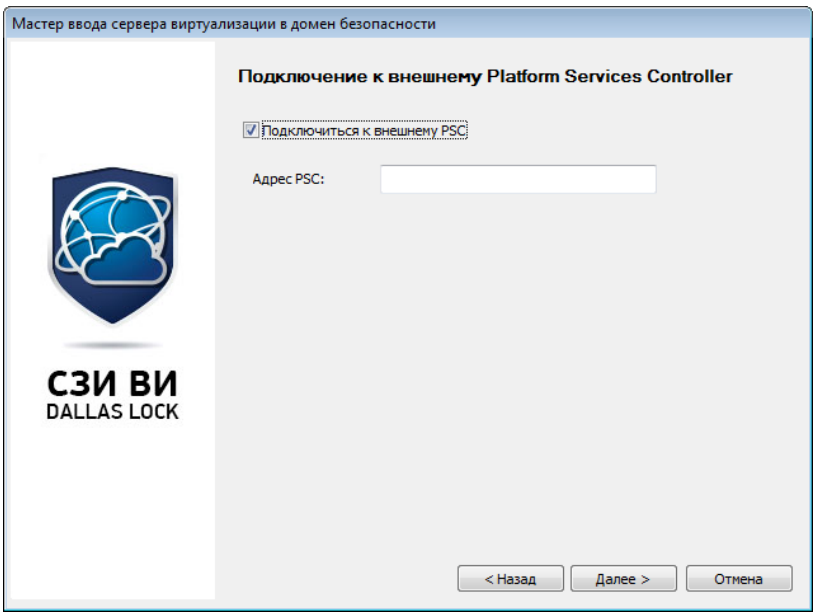


Рис. 45 – Ввод имени или IP-адреса сервера PSC

Нажать кнопку «Далее».

2) Выбрать тип ОС, установленной на сервере PSC (рис. 46).

[11] Доступно только для редакции «Расширенная».

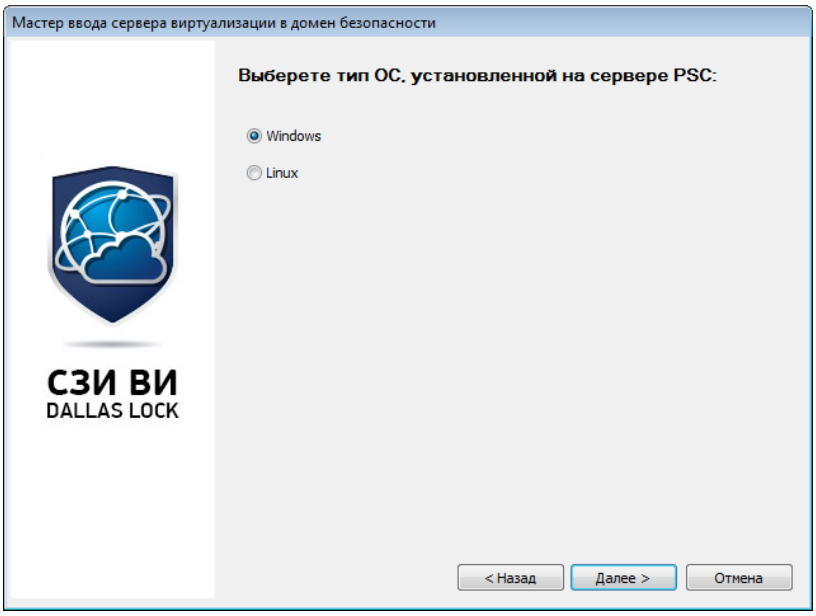


Рис. 46 – Выбор типа ОС, установленной на сервере PSC

Нажать кнопку «Далее».

3) Ввести учетные данные администратора сервера PSC в зависимости от выбранной ОС (рис. 47, рис. 48).

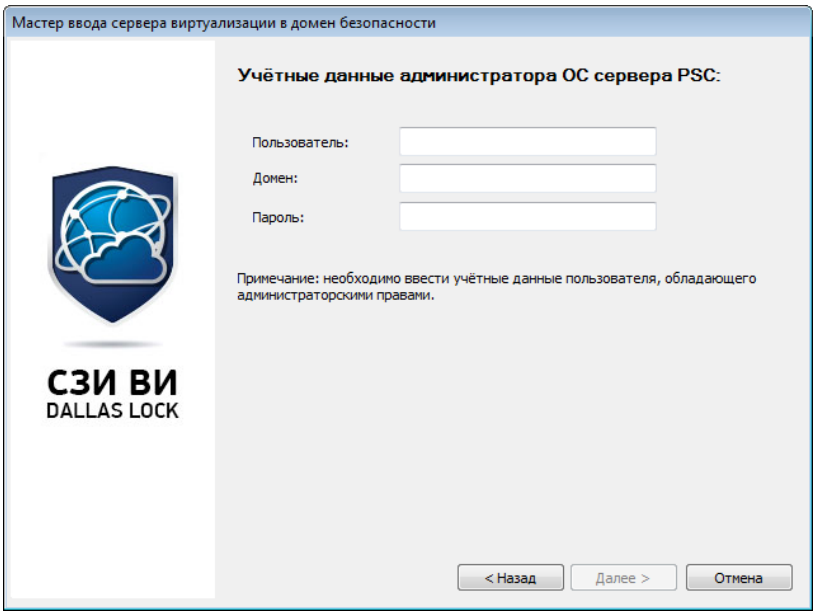


Рис. 47 – Ввод учетных данных администратора ОС Windows сервера PSC

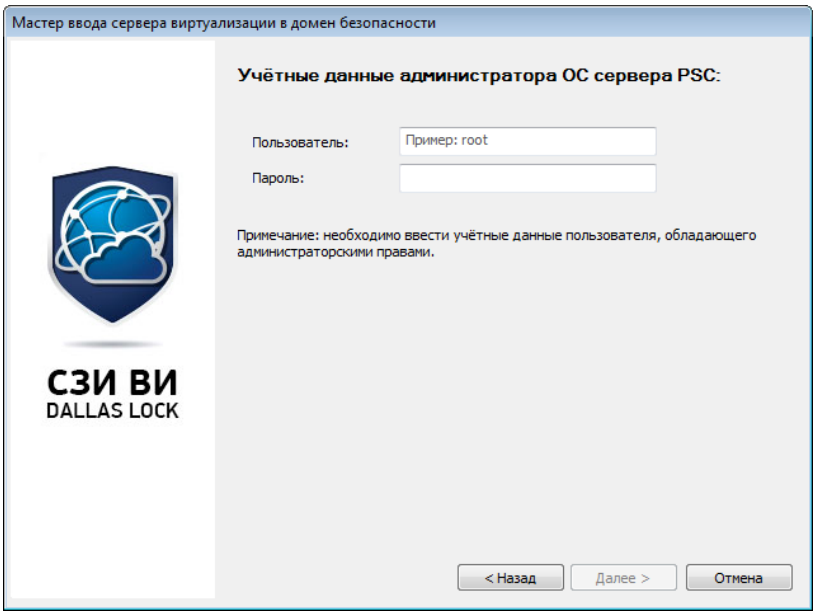


Рис. 48 – Ввод учетных данных администратора ОС Linux сервера PSC

11. После ввода учетных данных нажать кнопку «Далее».

12. Нажать кнопку «Завершить».

Запустится процесс подключения к серверу виртуализации и после успешного выполнения процедуры в дереве ВИ в поддереве vSphere появится объект нового СВ. Также соответствующий windows-клиент появится в дереве Агентом Windows в группе «СЗИ ВИ».

2.6.1.3 Установка агента DL ESXi на гипервизоре ESXi

Порядок установки и удаления агента DL ESXi на гипервизоре ESXi указан в п. 2.5.2.4 «Установка и удаление агента DL ESXi на гипервизоре ESXi».

2.6.2 Развертывание СЗИ ВИ для VMware vSphere vCSA

2.6.2.1 Установка компонента «Центр управления СЗИ ВИ Dallas Lock»

Порядок установки компонента «Центр управления СЗИ ВИ Dallas Lock» указан в п. 2.5.1 «Установка компонента «Центр управления СЗИ ВИ Dallas Lock»».

2.6.2.2 Ввод в домен безопасности и удаленная установка агента DL vCSA на сервер виртуализации с помощью мастера

Внимание! Перед установкой агента DL vCSA необходимо проверить срок действия пароля root. При истекшем сроке действия пароля root для vCSA установка агента DL vCSA не будет осуществлена.

Для ввода в домен безопасности и установки агента DL vCSA необходимо:

1. Запустить Консоль.

2. Во вкладке «Агенты ВИ» выбрать уровень «Сервер УД» и открыть вкладку «Состояние».

3. В блоке «Действия с ВИ» нажать кнопку «Добавить сервер виртуализации» (см. рис. 39).

4. В появившемся информационном окне нажать кнопку «Далее».

5. Ввести IP-адрес или полное доменное имя сервера виртуализации и нажать кнопку «Далее» (рис. 40).

Внимание! В случае, если IP-адрес сервера виртуализации vCSA является динамическим, его DNS-имя не должно содержать кириллические символы.

6. Выбрать тип агента VMware vCenter Server Appliance (рис. 41).

7. Выбрать способ установки агента:

- VMware API – в случае, если VCSA развернут как виртуальная машина на гипервизоре (т.н. вложенная виртуализация);
- SSH + SFTP – в случае, если VCSA развернут на локальной машине.

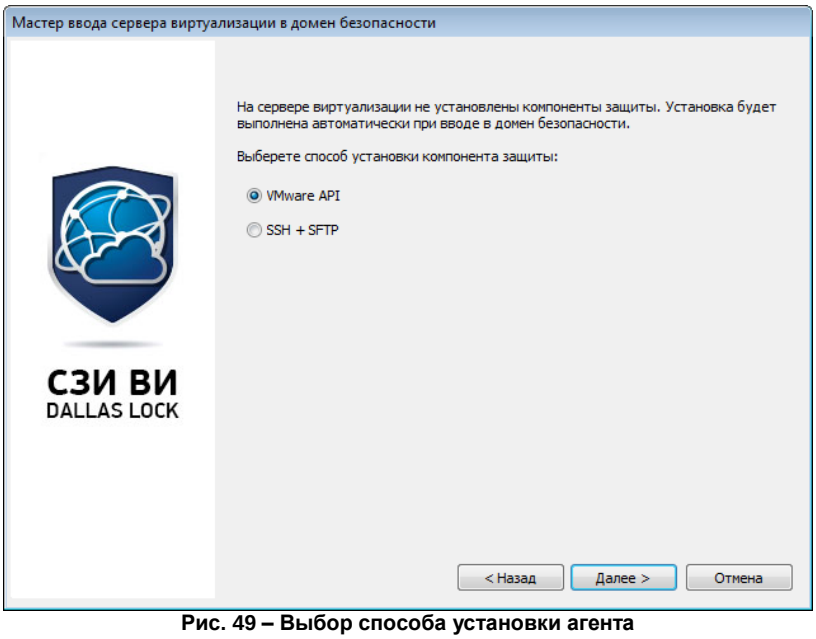


Рис. 49 – Выбор способа установки агента

Примечание. В случае ошибки установки агента vCSA попробуйте переключить способ установки агента на другой.

Примечание. Метод установки «VMware API» не работает, если хост ESXi, на котором развернута ВМ с vCSA, не введен в vCSA.

8. Ввести учетные данные администратора vSphere (рис. 44).

Нажать кнопку «Далее».

9. При наличии внешнего Platform Service Controller (PSC)[12].

1) Если требуется подключение к внешнему необходимо установить флаг в поле «Подключиться к внешнему PSC» и ввести IP-адрес или полное доменное имя сервера (рис. 45).

   Нажать кнопку «Далее».

2) Выбрать тип ОС, установленной на сервере PSC (рис. 46).

   Нажать кнопку «Далее».

3) Ввести учетные данные администратора сервера PSC (рис. 47).

   Нажать кнопку «Далее».

10. Нажать кнопку «Завершить».

Запустится процесс подключения к серверу виртуализации и после успешного выполнения процедуры в дереве ВИ в поддереве vSphere появится объект нового СВ.

2.6.2.3 Установка агента DL ESXi на гипервизоре ESXi

Порядок установки и удаления агента DL ESXi на гипервизоре ESXi указан в п. 2.5.2.4 «Установка и удаление агента DL ESXi на гипервизоре ESXi».

2.6.3 Развертывание СЗИ ВИ для Hyper-V

2.6.3.1 Установка компонента «Центр управления СЗИ ВИ Dallas Lock»

Порядок установки компонента «Центр управления СЗИ ВИ Dallas Lock» указан в п. 2.5.1 «Установка компонента «Центр управления СЗИ ВИ Dallas Lock»».

2.6.3.2 Ввод в домен безопасности и удаленная установка агента DL Hyper-V на сервер виртуализации с помощью мастера

Для ввода в домен безопасности и установки агента DL Hyper-V необходимо:

[12] Доступно только для редакции «Расширенная».

1. Запустить Консоль.
2. Во вкладке «Агенты ВИ» выбрать уровень «Сервер УД» и открыть вкладку «Состояние».
3. В блоке «Действия с ВИ» нажать кнопку «Добавить сервер виртуализации».
4. В появившемся информационном окне нажать кнопку «Далее».
5. Ввести IP-адрес или полное доменное имя сервера виртуализации и нажать кнопку «Далее».
6. Выбрать тип агента Microsoft Hyper-V/SC VMM.

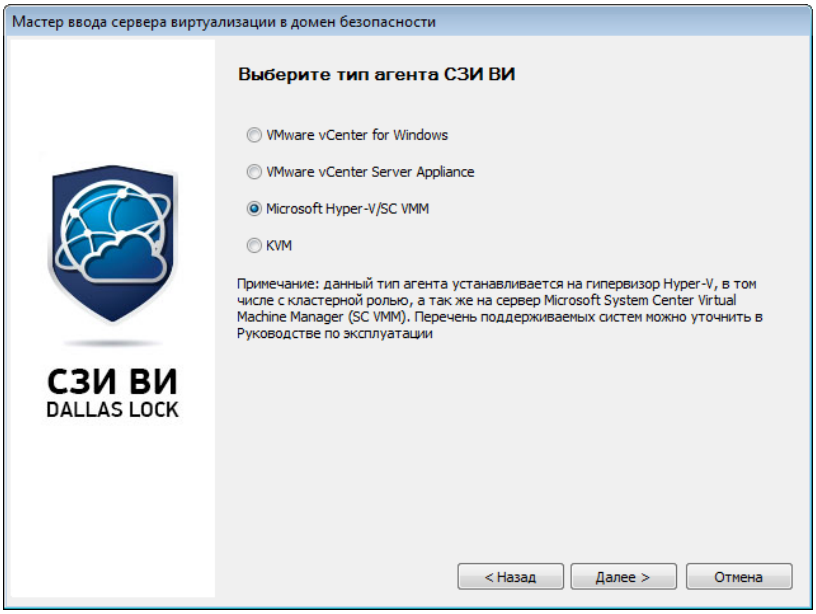


Рис. 50 – Выбор типа устанавливаемого агента

Нажать кнопку «Далее».

7. Ввести учетные данные администратора ОС.

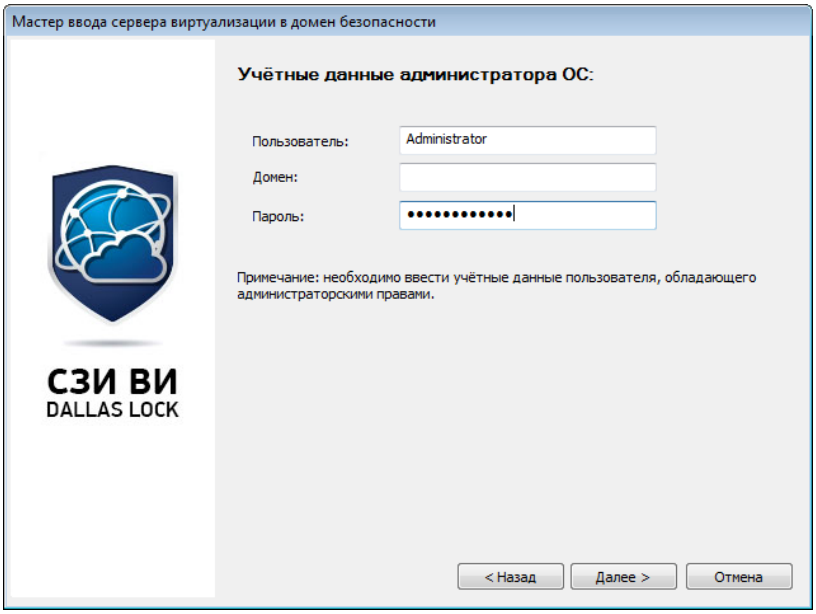


Рис. 51 – Ввод данных администратора ОС

Нажать кнопку «Далее».

8. Если требуется удаленная установка агента DL[13] на СВ необходимо установить флаг в поле «Установить компоненты защиты» (рис. 43).

В активировавшиеся поля ввести следующие данные:

- номер лицензии;
- код технической поддержки;
- ключ доступа к СУД (подробнее см. п. 5.6 «Ключи удаленного доступа»).

[13] Без установленных компонентов защиты ввод в домен безопасности невозможен.

Указать путь к дистрибутиву СЗИ ВИ.

Если требуется перезагрузить СВ после установки компонентов защиты и вывести сообщение для пользователей необходимо установить флаг в поле «Перезагрузить удаленный компьютер после установки» и заполнить необходимые поля.

Нажать кнопку «Далее».

9. При наличии кластерной роли необходимо выбрать соответствующий пункт.

Внимание! В домен безопасности будет добавлен только один узел кластера. Остальные узлы кластера необходимо добавлять отдельно.

Нажать кнопку «Далее».

10. Нажать кнопку «Завершить».

Запустится процесс подключения к серверу виртуализации и после успешного выполнения процедуры в дереве ВИ в поддереве Hyper-V появится объект нового СВ. Также соответствующий windows-клиент появится в дереве Агентом Windows в группе «СЗИ ВИ».

В случае, если СВ Hyper-V добавлялся с кластерной ролью, в дереве ВИ в поддереве Hyper-V будет создан специальный объект Кластера Hyper-V с соответствующим именем. Объект нового СВ Hyper-V с кластерной ролью в свою очередь будет добавлен в поддерево объекта Кластера.

Внимание! СЗИ ВИ «Dallas Lock» поддерживает управление серверами Hyper-V через System Center Virtual Machine Manager и Failover Cluster Manager, при этом следует учитывать, что в режиме использования данных инструментов управления кластеризацией типовые операции могут отличаться от выполняемых операций, вызванных через Консоль ЦУ СЗИ ВИ.

2.6.4 Развертывание СЗИ ВИ для KVM

2.6.4.1 Установка компонента «Центр управления СЗИ ВИ Dallas Lock»

Порядок установки компонента «Центр управления СЗИ ВИ Dallas Lock» указан в п. 2.5.1 «Установка компонента «Центр управления СЗИ ВИ Dallas Lock»».

2.6.4.2 Ввод в домен безопасности и удаленная установка агента DL KVM на сервер виртуализации с помощью мастера

Перед установкой агента DL KVM, необходимо убедиться, что к гипервизору открыт доступ по SSH и отключена политика «Вход: блокировать протокол SSH» (подробнее см. п.5.3.1.3 «Параметры входа для KVM/oVirt/zVirt/HOSTVM»). Далее для ввода в домен безопасности и установки агента DL KVM необходимо:

1. Запустить Консоль.

2. Во вкладке «Агенты ВИ» выбрать уровень «Сервер УД» и открыть вкладку «Состояние».

3. В блоке «Действия с ВИ» нажать кнопку «Добавить сервер виртуализации».

4. В появившемся информационном окне нажать кнопку «Далее».

5. Ввести IP-адрес или полное доменное имя сервера виртуализации и нажать кнопку «Далее».

6. Выбрать тип агента KVM.

Нажать кнопку «Далее».

7. Диалоговое окно с выбором инфраструктуры oVirt и вводом учетных данных необходимо пропустить, нажав кнопку «Далее».

8. Ввести учетные данные администратора ОС.

9. Нажать кнопку «Завершить».

2.6.5 Развертывание СЗИ ВИ для oVirt/zVirt/HOSTVM/РЕД Вирт

2.6.5.1 Установка компонента «Центр управления СЗИ ВИ Dallas Lock»

Порядок установки компонента «Центр управления СЗИ ВИ Dallas Lock» указан в п. 2.5.1 «Установка компонента «Центр управления СЗИ ВИ Dallas Lock»».

2.6.5.2 Ввод в домен безопасности и удаленная установка агента DL Engine на сервер

виртуализации с помощью мастера

Перед установкой агента DL Engine, необходимо убедиться, что к СВ открыт доступ по SSH и отключена политика «Вход: блокировать протокол SSH» (подробнее см. п. 5.3.1.3 «Параметры входа для KVM/oVirt/zVirt/HOSTVM/РЕД Вирт»).

Далее для ввода в домен безопасности и установки агента DL Engine необходимо:

1. Запустить Консоль.
2. Во вкладке «Агенты ВИ» выбрать уровень «Сервер УД» и открыть вкладку «Состояние».
3. В блоке «Действия с ВИ» нажать кнопку «Добавить сервер виртуализации».
4. В появившемся информационном окне нажать кнопку «Далее».
5. Ввести IP-адрес или полное доменное имя сервера виртуализации и нажать кнопку «Далее».
6. Выбрать тип агента KVM (рис. 52).

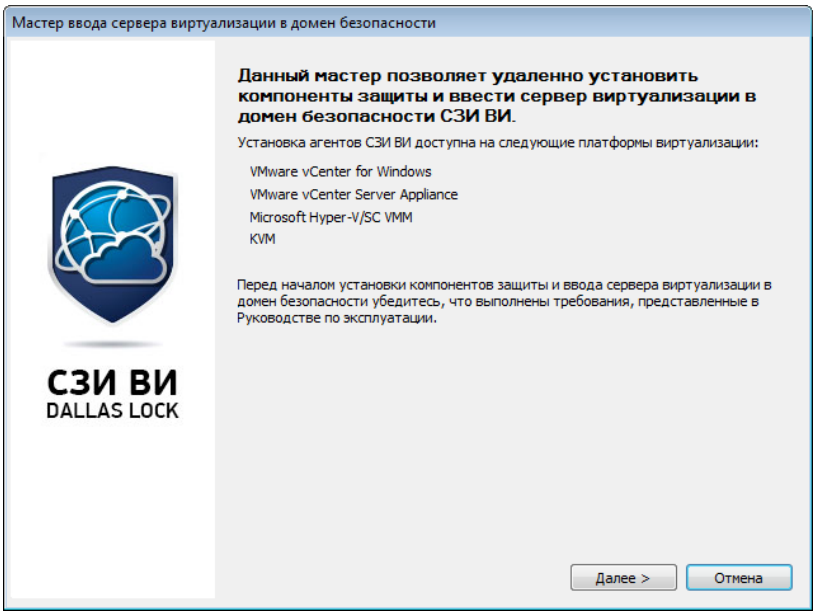


Рис. 52 – Выбор типа устанавливаемого агента

Нажать кнопку «Далее».

7. Ввести учетные данные администратора ОС.
8. Поставить флаг в поле «Виртуальная инфраструктура oVirt» и ввести учетные данные администратора системы виртуализации oVirt/zVirt/HOSTVM/РЕД Вирт[14].
9. Нажать кнопку «Завершить».

Если операция завершилась успешно, то в дереве «Агенты ВИ» появятся значки новых объектов ВИ.

Для удаления СВ из домена безопасности и агента DL Engine необходимо в категории действия нажать кнопку «Удалить из ВИ».

Примечание. В случае необходимости возможно удалить агент DL Engine локально вручную. Для этого следует в командной строке выполнить команду "/opt/confident/bin/uninstall_agent.sh".

2.6.5.3 Установка и удаление агента DL Host на гипервизоре oVirt/zVirt/HOSTVM/РЕД Вирт

Порядок установки и удаления агента DL Host на гипервизоре oVirt/zVirt/HOSTVM/РЕД Вирт указан в п. 2.5.6.3 «Установка и удаление агента DL Host на гипервизоре ».

2.7 Установка учетных данных

Установка учетных данных для введенных в ДБ СВ и гипервизоров необходима в случаях смены данных учетной записи администратора объекта ВИ, изменении разрешений, списков пользователей и прочих локальных параметров.

[14] Поддерживается только встроенный домен (internal).

2.7.1 Установка учетных данных для vSphere

Чтобы установить учетные данные для СВ необходимо на уровне СВ в блоке «Действия» либо через контекстное меню нажать кнопку «Установить учетные данные». В появившемся окне необходимо ввести данные пользователя и установить флаг в поле «Обновить данные с сервера» (рис. 53). Затем нажать кнопку «ОК».

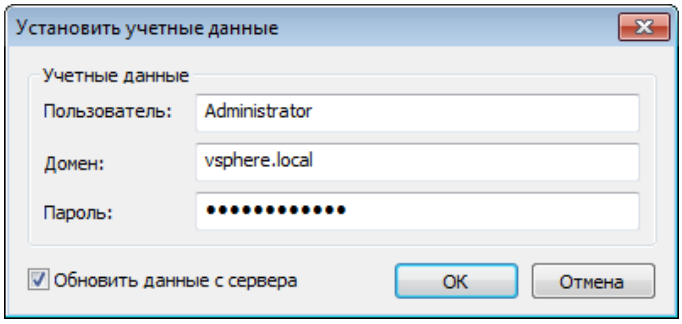


Рис. 53 – Установка учетных на данных на примере СВ vCenter

2.7.1.1 Установка учетных данных для гипервизора ESXi

Установка учетных данных для гипервизора описана в п. 2.5.2.4 «Установка и удаление агента DL ESXi на гипервизоре ESXi». Устанавливать флаг «Установить агент DL на гипервизоре» на 5 шаге не требуется.

2.7.2 Установка учетных данных для гипервизора KVM

Перед установкой учетных данных для гипервизора KVM, необходимо убедиться, что к гипервизору открыт доступ по SSH и отключена политика «Вход: блокировать протокол SSH» (подробнее см. п. 5.3.1.3 «Параметры входа для KVM/oVirt/zVirt/HOSTVM/РЕД Вирт»).

Чтобы установить учетные данные для гипервизора необходимо на уровне гипервизора в блоке «Действия» либо через контекстное меню нажать кнопку «Установить учетные данные». В появившемся окне необходимо ввести данные пользователя и установить флаг в поле «Обновить данные с сервера» (рис. 54). Затем нажать кнопку «ОК».

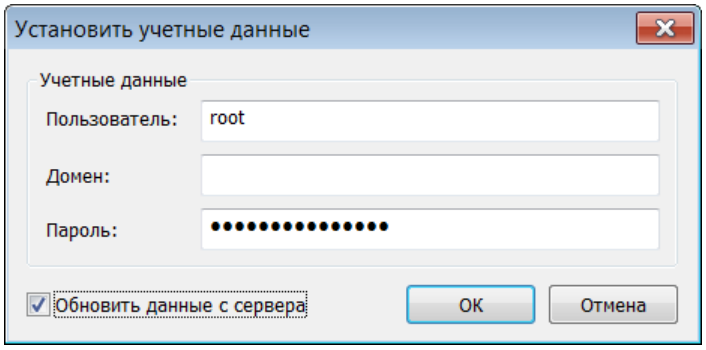


Рис. 54 – Установка учетных на данных гипервизора KVM

2.7.3 Установка учетных данных для СВ oVirt/zVirt/HOSTVM/РЕД Вирт

Чтобы установить учетные данные для СВ необходимо на уровне СВ в блоке «Действия» либо через контекстное меню нажать кнопку «Установить учетные данные». В появившемся окне необходимо ввести данные пользователя и установить флаг в поле «Обновить данные с сервера» (рис. 55). Затем нажать кнопку «ОК».

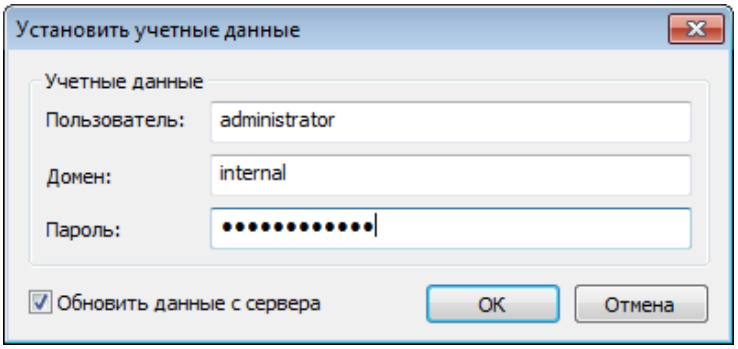


Рис. 55 – Установка учетных на данных СВ oVirt/zVirt/HOSTVM/РЕД Вирт

2.7.3.1 Установка учетных данных для гипервизора oVirt/zVirt/HOSTVM/РЕД Вирт

Перед установкой учетных данных для гипервизора oVirt/zVirt/HOSTVM, необходимо убедиться, что к гипервизору открыт доступ по SSH и отключена политика «Вход: блокировать протокол SSH» (подробнее см. п. 5.3.1.3 «Параметры входа для KVM/oVirt/zVirt/HOSTVM»).

Чтобы установить учетные данные для гипервизора необходимо на уровне гипервизора в блоке «Действия» либо через контекстное меню нажать кнопку «Установить учетные данные». В появившемся окне необходимо ввести данные пользователя и установить флаг в поле «Обновить данные с сервера» (рис. 56). Затем нажать кнопку «ОК».

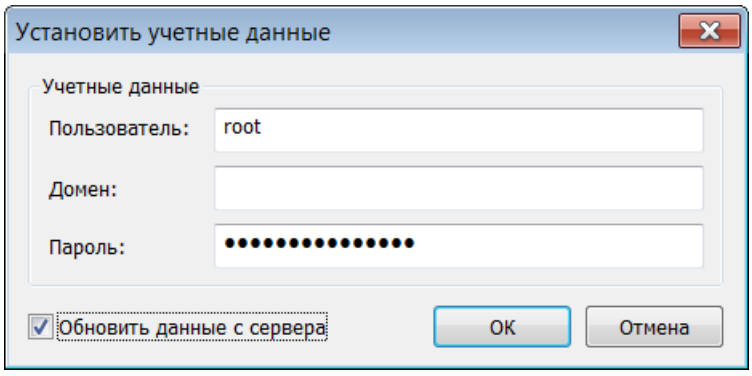


Рис. 56 – Установка учетных на данных гипервизора oVirt/zVirt/HOSTVM/РЕД Вирт

2.8 Вывод серверов виртуализации из домена безопасности

Для вывода сервера виртуализации из домена безопасности необходимо:

1) Открыть дерево «Агенты ВИ».
2) Выбрать уровень Сервера виртуализации и открыть категорию «Состояние» → «Основное».
3) Нажать кнопку «Удалить из ВИ» в блоке «Действия» или воспользоваться контекстным меню (рис. 57).

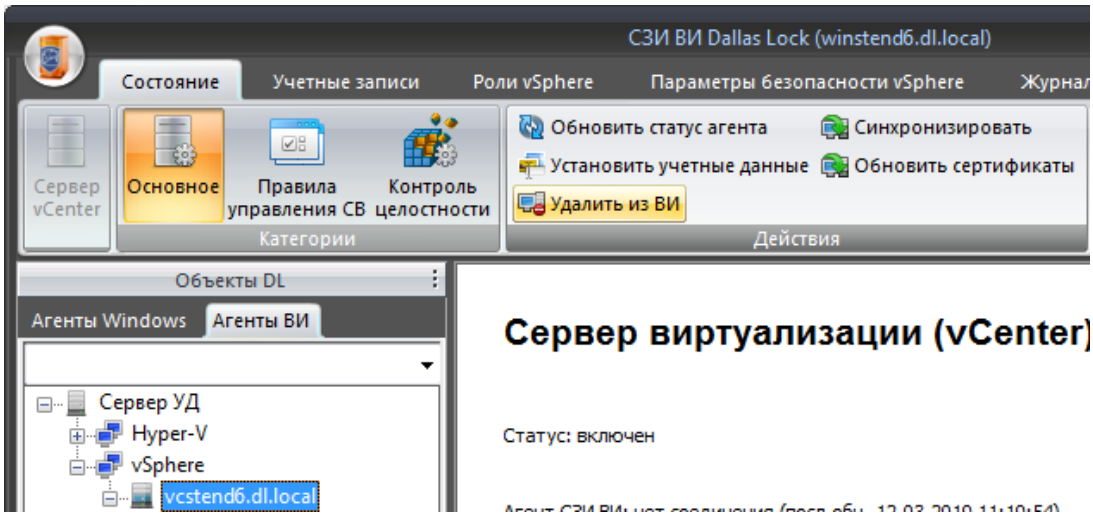


Рис. 57 – Удаление сервера виртуализации из ВИ с Консоли

4) Подтвердить запрос на вывод сервера виртуализации из домена, нажав кнопку «Да».

2.9 Удаление СЗИ ВИ

2.9.1 Удаление Центра управления СЗИ ВИ Dallas Lock

Перед удалением СЗИ ВИ рекомендуется сохранить файлы конфигурации ЦУ СЗИ ВИ (подробнее см. п. 11.1 «Сохранение конфигурации ЦУ СЗИ ВИ»).

Перед удалением компонентов СЗИ ВИ на СВ и ЦУ СЗИ ВИ необходимо завершить работу всех приложений и сохранить результаты, так как после удаления некоторых компонентов потребуется перезагрузка компьютера.

Удаление компонентов СЗИ ВИ производится с помощью Мастера установок. В разных операционных системах запуск Мастера установок может осуществляться по-разному. Например, в ОС Windows 7 необходимо открыть «Пуск» → «Панель управления» → «Программы и компоненты». В появившемся окне необходимо выбрать в списке пункт «SZVI Dallas Lock», нажать

кнопку «Удалить» и подтвердить удаление (рис. 58).

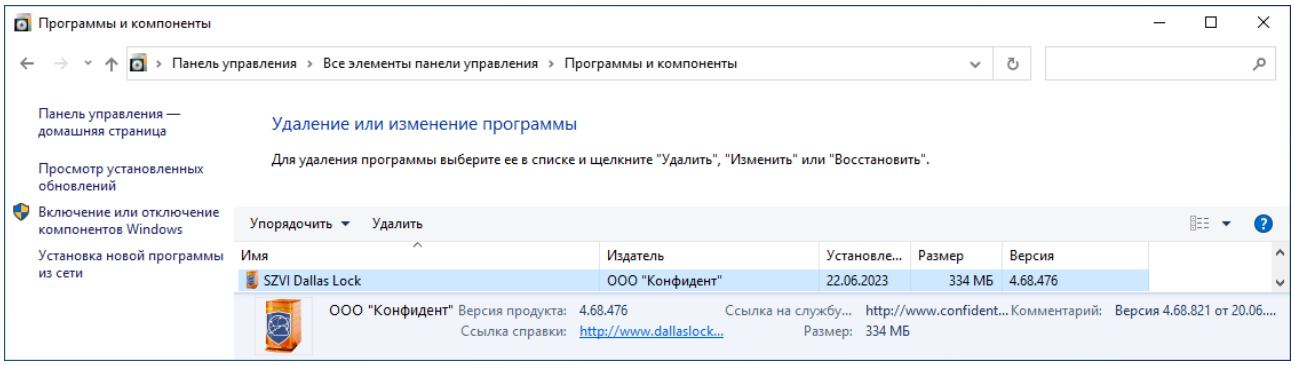


Рис. 58 – Удаление компонентов защиты

Если использовался механизм лицензирования через Сервер лицензий, при удалении Сервера УД зарезервированная квота на управление клиентами возвращается на Сервер лицензий.

После успешного удаления компонента защиты на СВ и ЦУ СЗИ ВИ появится информационное окно о необходимости перезагрузки ПК. В области уведомлений ОС Windows появится уведомление о том, что компьютер будет перезагружен через 1 минуту (рис. 59).

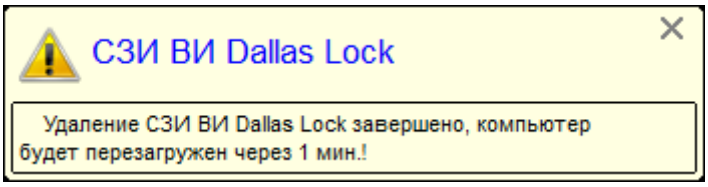


Рис. 59 – Уведомление об удалении СЗИ ВИ и перезагрузке компьютера

Внимание! При удалении Центр управления СЗИ ВИ Dallas Lock агенты DL ESXi и DL vCSA удаляются автоматически (если они были установлены и введены в домен безопасности).

2.9.2 Удаление агентов DL Windows

Удаление агентов DL Windows (агента vCenter for Windows или агента Hyper-V) возможно произвести двумя способами:

- локально;
- удаленно.

Для того, чтобы удалить агент локально, необходимо произвести на клиенте действия, описанные в п. 2.9.1 «Удаление Центра управления СЗИ ВИ Dallas Lock».

Примечание. Перед локальным удалением агента DL Hyper-V с компьютера, на котором ОС Windows Server 2012, 2012 R2, 2016 или 2019 была установлена в режиме «Server Core», необходимо убедиться, что в ОС запущен хотя бы один экземпляр консоли.

Чтобы произвести данную процедуру удаленно, необходимо:

1. В Консоли перейти в дерево «Агенты Windows».
2. Перейти на уровень клиента, с которого необходимо удалить агент. Вызвать контекстное меню и выбрать пункт «Удалить агенты DL Windows» (рис. 60).

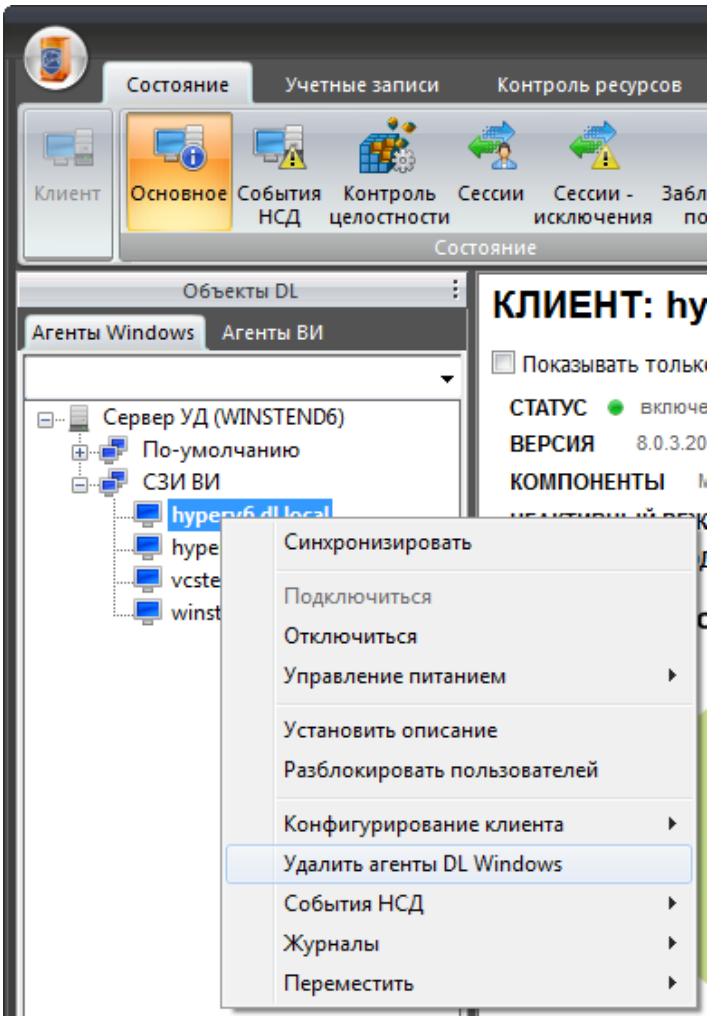


Рис. 60 – Удаленное удаление агента DL Windows

3. В появившемся окне мастера удаления СЗИ ВИ агентов из списка компьютеров для удаленных операций выбрать тот, с которого необходимо удалить агент (рис. 61). Нажать кнопку «Продолжить».

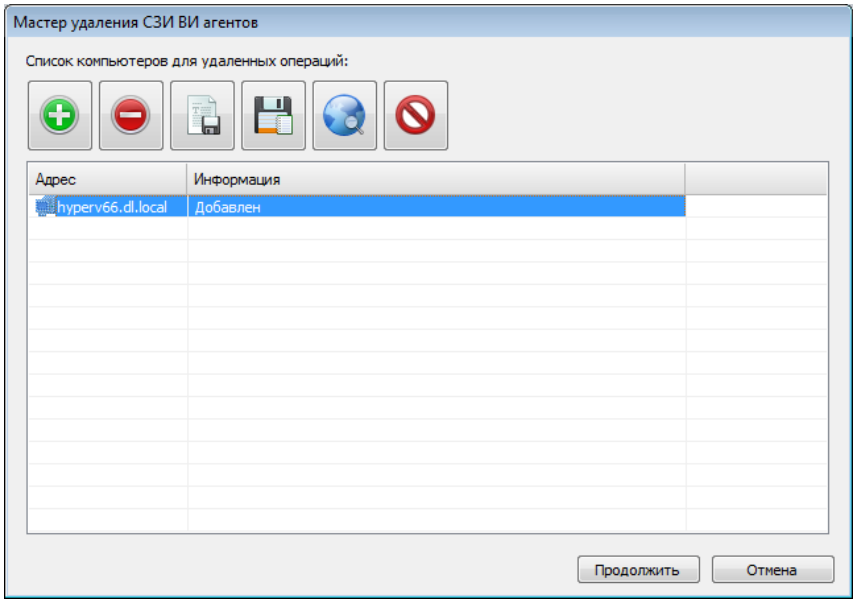


Рис. 61 – Мастер удаления СЗИ ВИ агентов

4. Далее необходимо ввести учетные данные администратора ОС компьютера клиента (рис. 62) и нажать кнопку «Продолжить».

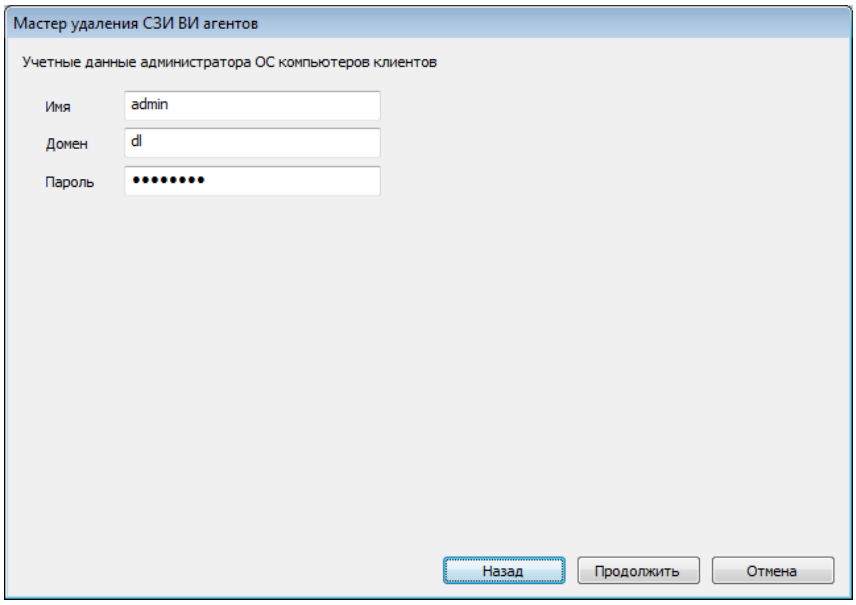


Рис. 62 – Ввод учетных данных администратора ОС компьютера клиента

5. В параметрах удаления клиентов можно инициализировать перезагрузку компьютера клиента после удаления агента DL Windows. Для этого необходимо поставить флаг в поле «Перезагрузить удаленный компьютер после удаления» (рис. 63). Нажать кнопку «Продолжить».

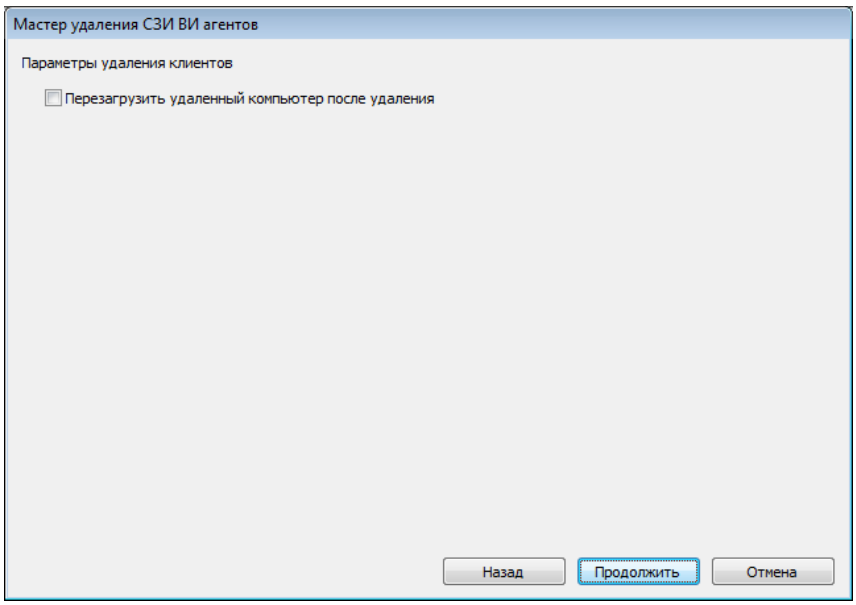


Рис. 63 – Перезагрузка компьютера клиента

В случае, если удаленную перезагрузку компьютера клиента решено не производить, его необходимо будет позже перезагрузить вручную.

6. В мастере удаления СЗИ ВИ агентов отобразится процесс удаления агента DL Windows. В области уведомлений Windows отобразится сообщение об успешном удалении агента DL Windows (рис. 64). После этого необходимо нажать кнопку «Завершить» в окне Мастера удаления СЗИ ВИ агентов.

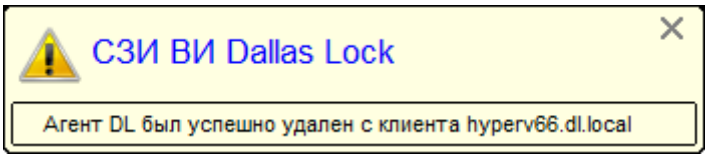


Рис. 64 – Сообщение об удалении агента DL Windows

2.9.3 Удаление агента DL ESXi

Для удаления агента DL ESXi, необходимо в категории действия нажать кнопку «Удалить агент DL на гипервизоре», либо вызвать щелчком правой кнопки мыши на гипервизоре контекстное меню и выбрать соответствующий пункт.

Примечание. В случае необходимости возможно удалить агент DL ESXi локально вручную. Для этого следует в командной строке выполнить команду "esxcli software vib remove -f -n confident-agentd".

2.9.4 Удаление агента DL vCSA

Для удаления агента DL vCSA, необходимо на уровне Сервера виртуализации в категории «Основное» нажать кнопку «Удалить из ВИ» (рис. 65) или воспользоваться контекстным меню.

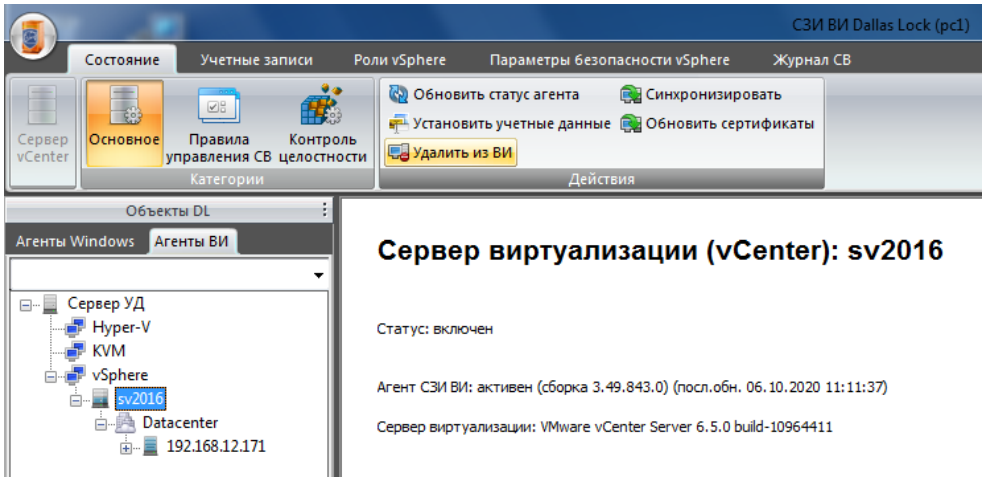


Рис. 65 – Удаление агента DL vCSA

Примечание. В случае необходимости, можно осуществить аварийное удаление агента DL vCSA, выполнив в командной строке СВ команду "rpm -e confident-agentd".

2.9.5 Удаление агента DL KVM

Для удаления агента DL KVM, необходимо на уровне Сервера виртуализации в категории «Основное» нажать кнопку «Удалить из ВИ» (рис. 66) или воспользоваться контекстным меню.

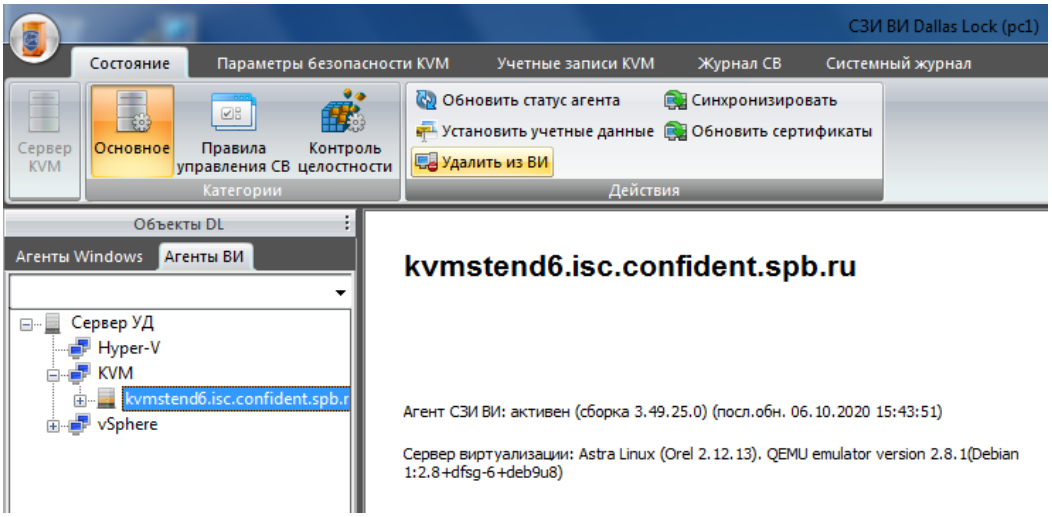


Рис. 66 – Удаление агента DL KVM

Примечание. В случае необходимости, можно осуществить аварийное удаление агента DL KVM, выполнив в командной строке гипервизора команду "/opt/confident/bin/uninstall_agent.sh".

2.9.6 Удаление агентов DL oVirt/zVirt/HOSTVM/РЕД Вирт

Удаление агента DL Engine

Для удаления агента DL Engine, необходимо на уровне Сервера виртуализации в категории «Основное» нажать кнопку «Удалить из ВИ» или воспользоваться контекстным меню.

Удаление агента DL Host

Для удаления агента DL Host, необходимо на уровне гипервизора в категории «Основное» нажать кнопку «Удалить агент DL на гипервизоре» или воспользоваться контекстным меню.

Примечание. В случае необходимости, можно осуществить аварийное удаление агентов DL Host и DL Engine, выполнив в командной строке гипервизора/СВ команду "/opt/confident/bin/uninstall_agent.sh".

2.10 Обновление системы защиты

Перед установкой обновленного дистрибутива необходимо выполнить проверку подлинности электронной подписи (согласно инструкции, представленной на сайте www.dallaslock.ru) и расчет и сверку контрольных сумм полученного пакета обновлений с контрольными суммами, указанными на сайте.

Информация о появлении обновленной версии СЗИ ВИ отображается на сайте www.dallaslock.ru.

Так же реализован механизм проверки наличия более новых версий СЗИ ВИ с использованием открытого канала связи (протокол http).

Для проверки наличия обновления необходимо выполнить следующие действия:

1. Открыть дополнительное меню Консоли и нажать кнопку «О программе».
2. В появившемся окне нажать кнопку «Проверить обновление».
3. Будет произведена проверка наличия обновления. В открывшемся окне будет отображено сообщение о результатах проверки.

Для получения обновления необходимо выполнить следующие действия:

1. Обратиться в службу технической поддержки ООО «Конфидент» (обновление предоставляется только при наличии действующей (оплаченной) технической поддержки).
2. Получить от сотрудника технической поддержки ООО «Конфидент» ссылку на архив, расположенный на ftp-сервере ООО «Конфидент». Архив содержит в себе обновленный дистрибутив СЗИ ВИ.
3. Сохранить и распаковать указанный архив на жесткий диск ПК (либо на другой накопитель), на котором требуется обновить СЗИ ВИ.

2.10.1 Стандартное обновление

Обновление установленной системы защиты выполняется путем удаления СЗИ ВИ и ее компонентов защиты с объектов ВИ и клиентов windows (подробнее см. п. 2.2 «Ограничения при установке и эксплуатации» и 2.9 «Удаление СЗИ ВИ») и установки обновленного дистрибутива с последующей установкой агентов DL (подробнее см. п. 2.5 «Развертывание СЗИ ВИ»).

Перед удалением рекомендуется воспользоваться функцией сохранения конфигурации предыдущей версии СЗИ ВИ (подробнее см. п. 11.1 «Сохранение конфигурации ЦУ СЗИ ВИ»).

Внимание! Сохранение и применение файла конфигурации ЦУ СЗИ ВИ осуществляется только на соответствующем ЦУ СЗИ ВИ с соответствующей версией, на котором данная конфигурация была сформирована. Использовать данный механизм для обновления СЗИ ВИ на более старшую версию не рекомендуется.

2.10.2 Обновление windows-клиентов с помощью программы обновления

Внимание! Данный способ возможно применять только для windows-клиентов (ТС с установленным ЦУ СЗИ ВИ, СВ vCenter и Hyper-V) с предварительным удалением компонентов защиты СЗИ ВИ с объектов ВИ (гипервизоры ESXi, KVM и СВ vCSA).

Обновление установленной системы защиты выполняется в следующем порядке:

1. Перед удалением рекомендуется воспользоваться функцией сохранения конфигурации

предыдущей версии СЗИ ВИ (подробнее см. п. 11.1 «Сохранение конфигурации ЦУ СЗИ ВИ»).

2. Удалить компоненты защиты СЗИ ВИ с объектов ВИ - гипервизоры ESXi, KVM и СВ vCSA (подробнее см. п.2.9 «Удаление СЗИ ВИ»).
3. Скопировать файл SzviUpdater.exe в одну папку с устанавливаемым дистрибутивом на ТС, на котором будет производиться обновление (имя дистрибутива должно быть DLVI.msi).
4. Запустить SzviUpdater.exe. Будет произведено определение установленной и устанавливаемой версии СЗИ ВИ.

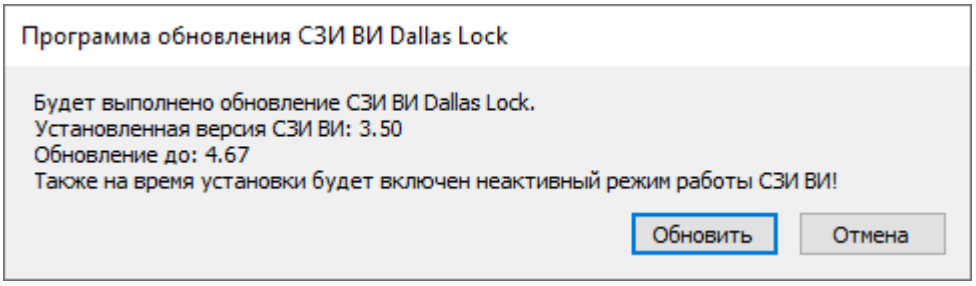


Рис. 67 – Обновление СЗИ ВИ

5. Нажать кнопку «Обновить».
6. Далее запуститься стандартный процесс установки, где при необходимости можно сменить номер лицензии и код технической поддержки (подробнее см. п. 2.5 «Развертывание СЗИ ВИ»).

Процедуру обновления необходимо провести только локально на каждом windows-клиенте в ручном режиме.

2.11 О программе

Со следующими сведениями о СЗИ ВИ можно ознакомиться в информационном окне «О программе», вызвав его из списка дополнительных функций кнопки главного меню (рис. 68):

- полное наименование и редакция СЗИ ВИ;
- номер и дата сборки ЦУ СЗИ ВИ;
- номер лицензии;
- код технической поддержки (если он вводится при установке либо в процессе эксплуатации СЗИ ВИ);
- дата завершения технической поддержки;
- активные компоненты (модули, на которые приобретена лицензия);
- адрес сайта компании-разработчика;
- адрес сайта продуктовой линейки Dallas Lock;
- адрес технической поддержки;
- номер телефона.

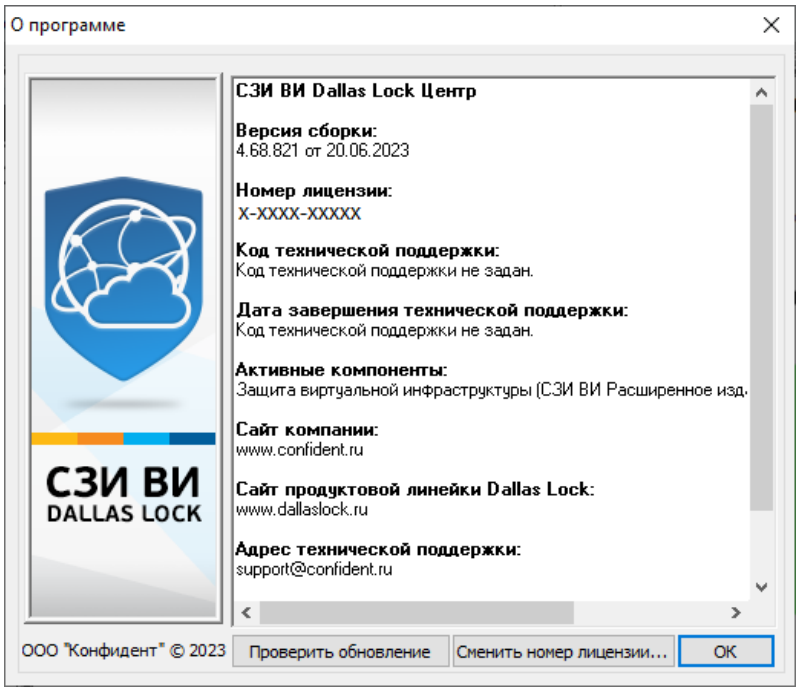


Рис. 68 – Окно «О программе»

Процесс обновления СЗИ ВИ с помощью кнопки «Проверить обновление» описан в п. 2.10 «Обновление системы защиты».

При установке без использования кода технической поддержки его необходимо ввести в процессе эксплуатации СЗИ ВИ: нажать кнопку «Сменить номер лицензии» и ввести код технической поддержки, также в появившемся окне можно изменить номер лицензии.

Действующий код технической поддержки является условием предоставления помощи в установке и настройке СЗИ ВИ специалистами компании-разработчика, а также условием доступа к сертифицированным обновлениям.

3 ОПИСАНИЕ СРЕДСТВ АДМИНИСТРИРОВАНИЯ

3.1 Консоль

Администрирование установленной СЗИ ВИ осуществляется из окна Консоли ЦУ СЗИ ВИ.

Вызов Консоли производится двойным щелчком мыши на ярлыке программы  на рабочем столе или в меню «Пуск». В окне подключения к ЦУ СЗИ ВИ требуется ввести следующие данные (рис. 69):

- имя ПК, на котором установлен Центр управления СЗИ ВИ Dallas Lock (автоматически отображается имя локального);
- имя учетной записи;
- домен (если это доменная учетная запись);
- предъявить и выбрать аппаратный идентификатор;
- пароль учетной записи пользователя.

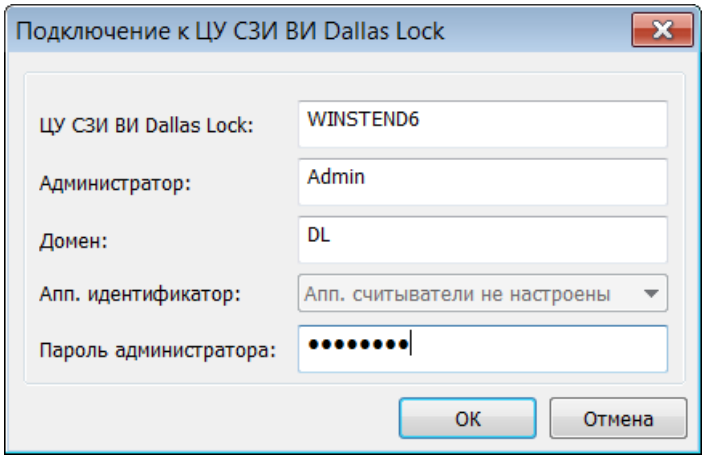


Рис. 69 – Ввод пароля учетной записи для входа в Консоль

Главное окно Консоли содержит следующие рабочие области (рис. 70):

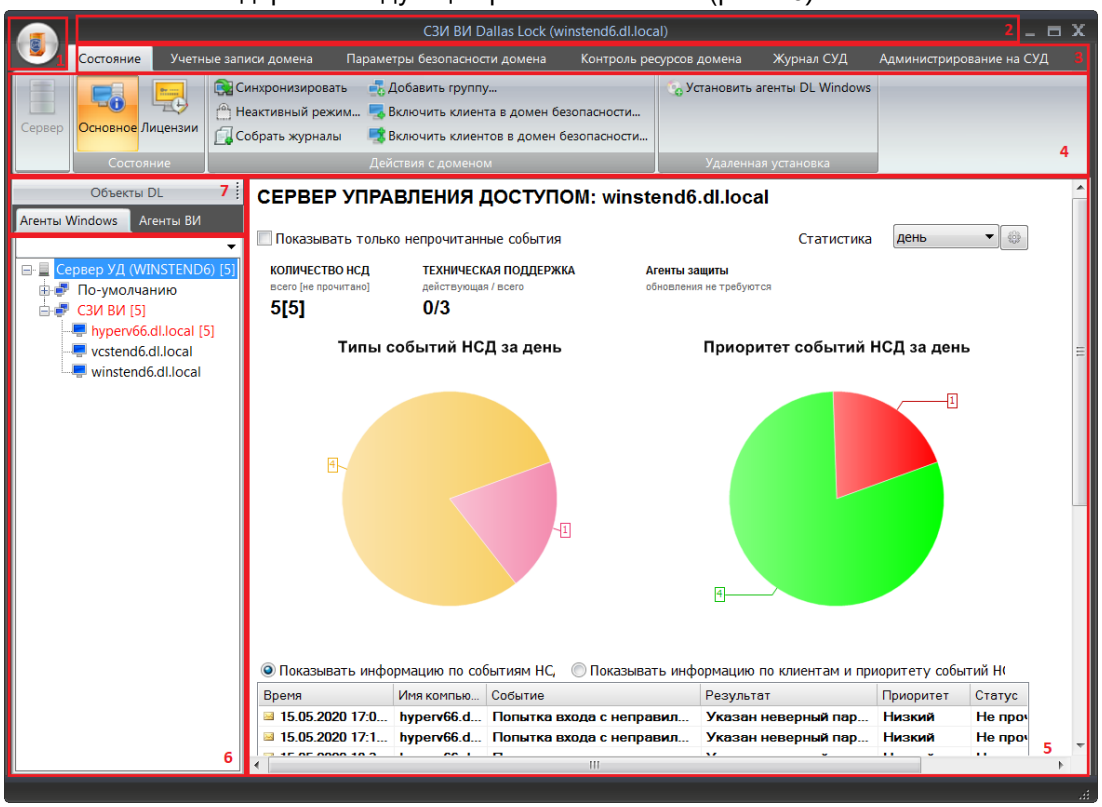


Рис. 70 – Окно Консоли

1. Кнопка дополнительного меню.

2. Заголовок окна (верхняя строка), содержащий название версии системы защиты, имя Сервера УД (по имени компьютера).
3. Основное меню с набором вкладок.
4. Категории параметров основного меню и панель действий.
5. Рабочая область, содержащая списки параметров или объектов текущей категории.
6. Проводник в виде дерева объектов, отображающий список клиентов, групп клиентов и объектов ВИ.
7. Вкладки выбора дерева (объектов DL).
8. Управление виртуальной инфраструктурой происходит в дереве «Агенты ВИ» (рис. 71).

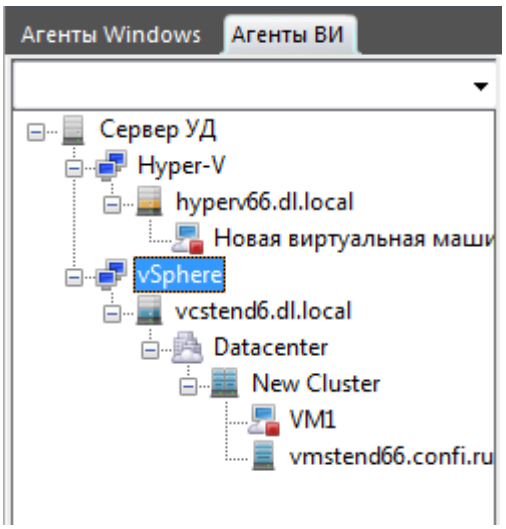


Рис. 71 – Объекты ВИ

С помощью Консоли можно настроить параметры безопасности для следующих объектов ВИ:

- — Сервер виртуализации Hyper-V;
- — Кластер Hyper-V
- — Сервер виртуализации KVM/oVirt/zVirt/HOSTVM/РЕД Вирт;
- — Сервер виртуализации vCenter/vCSA;
- — Дата центр;
- — Кластер хранилищ данных;
- — Хранилище данных;
- — Кластер гипервизоров;
- — Гипервизор;
- — Сеть виртуальных машин;
- — Распределенный коммутатор (dvSwitch);
- — Группа Uplink портов (dvUplinks);
- — Группа распределенных портов (dvPortGroup);
- — Виртуальная машина и ее состояние;
- — Шаблон виртуальной машины;
- — Виртуальный сервис (vApp);
- — Пул ресурсов (Resource pool);
- — Папка.

Для обновления дерева «Агенты ВИ» необходимо перейти на уровень Сервера УД в категорию «Состояние» → «Основное» и нажать кнопку «Обновить дерево» или выбрать соответствующий пункт из контекстного меню.

Для каждого из объектов в верхней части основного меню Консоли формируется свой список вкладок. При выборе вкладки в рабочей области открывается страница с соответствующими параметрами и меню.

Контекстное меню дерева Консоли позволяет на уровне Hyper-V добавлять Сервера виртуализации Hyper-V, на уровне vSphere добавлять сервера виртуализации vCenter и vCSA, на уровне KVM

добавлять гипервизоры KVM, СВ oVirt/zVirt/HOSTVM/РЕД Вирт и гипервизоры oVirt/zVirt/HOSTVM/РЕД Вирт и синхронизировать их по команде администратора ЦУ СЗИ ВИ.

3.2 Информационная панель

3.2.1 Дерево «Агенты Windows»

При выборе в дереве «Агенты Windows» корневого элемента «Сервер УД» в рабочей области отображается следующая информация (рис. 72) [15]:

1. наименование сервера УД;
2. опция выбора только непрочитанных событий НСД для отображения на круговых диаграммах (7) и в списке событий НСД (8);
3. количество событий НСД (зарегистрированных / не прочитанных);
4. информация о версии продукта и пакете технической поддержки;
5. информация об агентах защиты на клиентах;
6. блок выборки отображаемых данных по времени («день», «неделя», «месяц», «период»);
7. кнопка вызова настроек приоритетов и оформления круговых диаграмм;
8. круговые диаграммы (события НСД по типу и по приоритету);
9. список событий НСД с настройками сортировки и фильтрации.

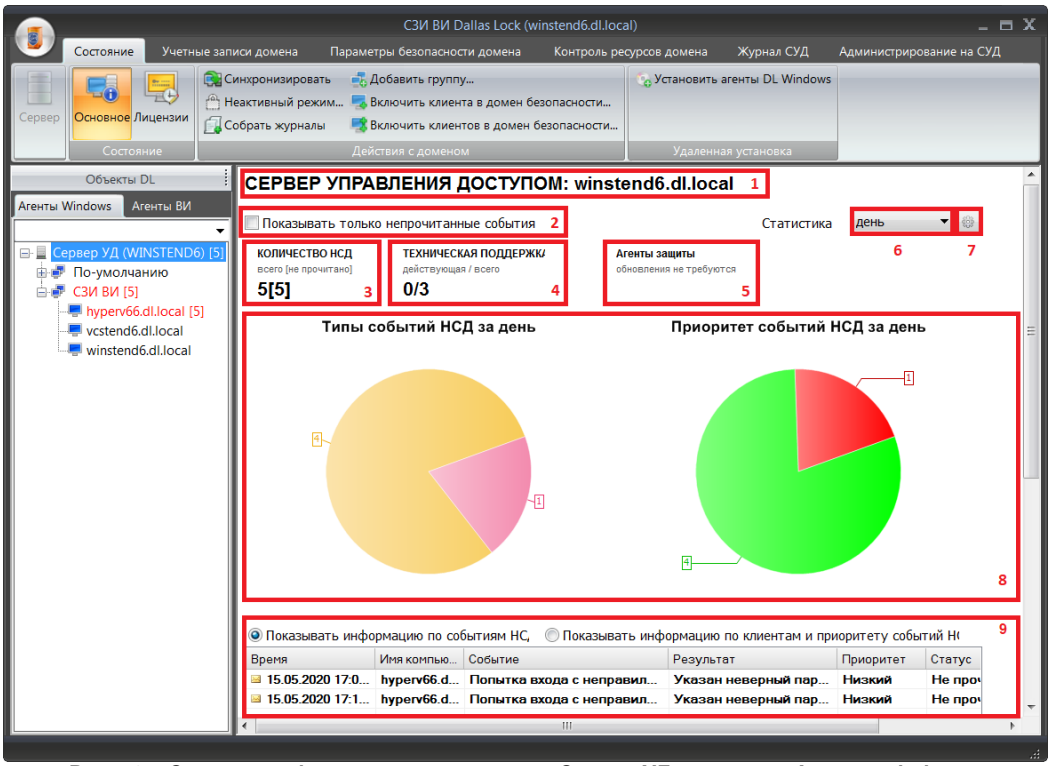


Рис. 72 – Сводная информация по элементу «Сервер УД» вкладки «Агенты Windows»

При нажатии на кнопку настроек приоритетов и оформления круговых диаграмм (6) откроется окно с настройками отображения типов событий по приоритетам[16] (рис. 73) и по цветам (рис. 74).

[15] В редакции «Стандартная» не отображаются элементы 2, 5, 6, 7, 8.

[16] Опция «Наследовать» не доступна для элемента «Сервер УД», см. п.3.8 «Наследование настроек».

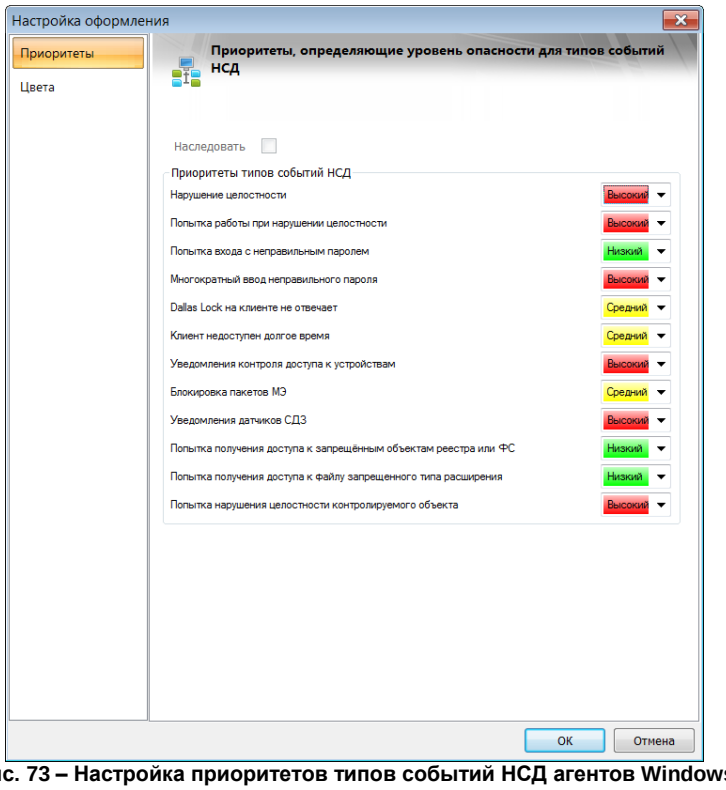


Рис. 73 – Настройка приоритетов типов событий НСД агентов Windows

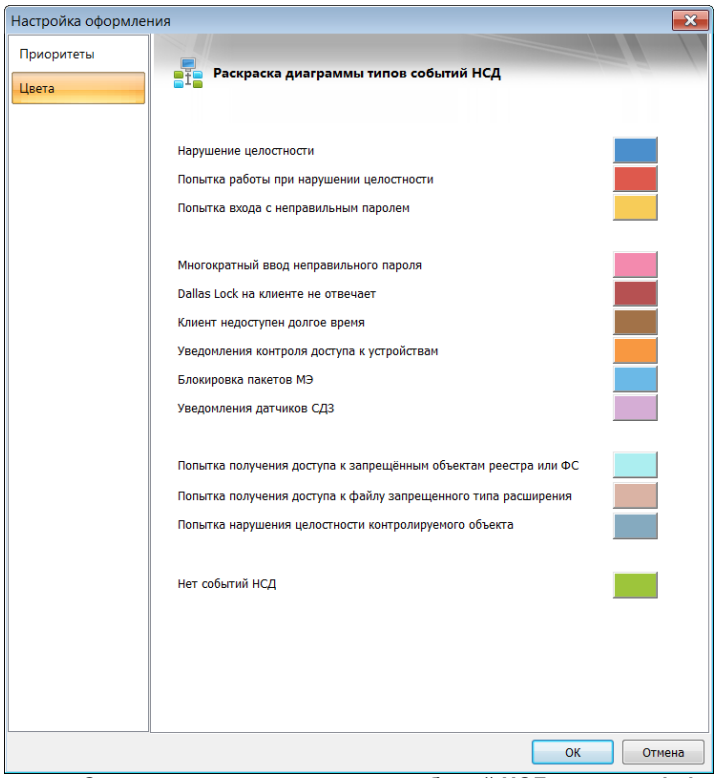


Рис. 74 – Сопоставление цветов типам событий НСД агентов Windows

Окна отображают перечень типов событий НСД, регистрация которых включена для Сервера УД. Для изменения перечня типов регистрируемых событий см. п. 3.6 «Сигнализация об НСД».

3.2.1.1 Информационная панель группы клиентов Windows

При выборе в дереве «Агенты Windows» группы клиентов в рабочей области отображается следующая информация (рис. 75):

1. наименование группы (1);
2. опция выбора только непрочитанных событий НСД для отображения на круговых диаграммах (2);

3. количество событий НСД (зарегистрированных / не прочитанных) (3);
4. количество лицензий технической поддержки (4);
5. информация об агентах защиты на клиентах (5);
6. блок выборки отображаемых данных по времени («день», «неделя», «месяц», «период») (6);
7. кнопка вызова настроек приоритетов и оформления круговых диаграмм (7);
8. круговые диаграммы (события НСД по типу и по приоритету) (8);
9. гистограмма (отображает количество событий НСД всех типов за выбранный период времени) (9);
10. список событий НСД с настройками сортировки и фильтрации (10).

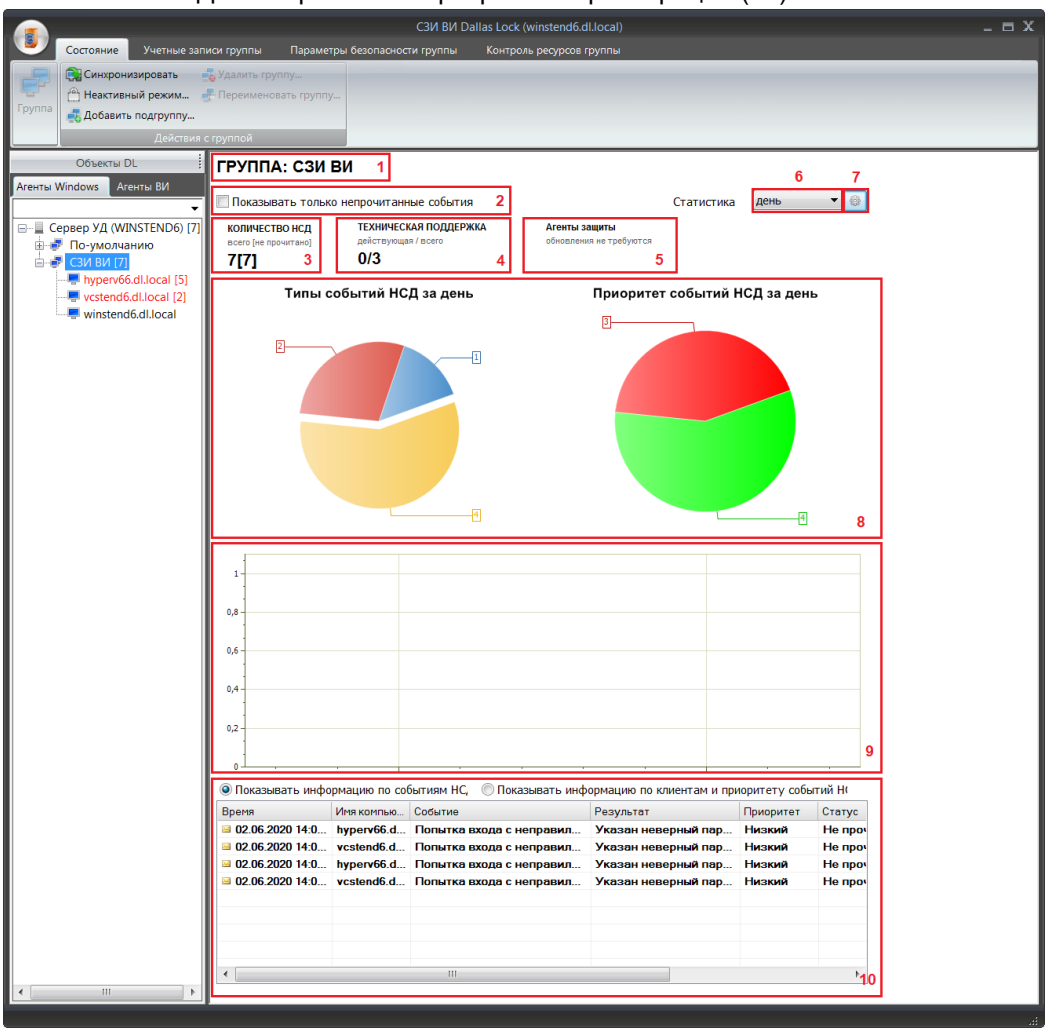


Рис. 75 – Сводная информация по группе клиентов Windows

Доступны следующие действия с группой:

- синхронизация параметров безопасности группы с ЦУ СЗИ ВИ (см. п. 3.5 «Синхронизация»);
- настройка неактивного режима (см. п. 3.7 «Неактивный режим»);
- добавить, удалить и переименовать группу (группы «По умолчанию» и «СЗИ ВИ» не редактируются).

3.2.1.2 Информационная панель клиента Windows

При выборе в дереве «Агенты Windows» клиента Windows в рабочей области отображается следующая информация (рис. 76)[17]:

1. имя клиента;
2. опция выбора только непрочитанных событий НСД для отображения на круговых диаграммах;
3. статус и версия агента DL;

[17] В редакции «Стандартная» не отображаются элементы 2, 9 ,10, 11, 12.

4. компоненты;
5. статус неактивного режима;
6. наличие технической поддержки продукта;
7. количество событий НСД (зарегистрированных / не прочитанных);
8. количество сессий на клиенте;
9. блок выборки отображаемых данных по времени («день», «неделя», «месяц», «период»);
10. кнопка вызова настроек приоритетов и оформления круговых диаграмм;
11. круговые диаграммы (события НСД по типу и по приоритету);
12. список событий НСД с настройками сортировки и фильтрации.

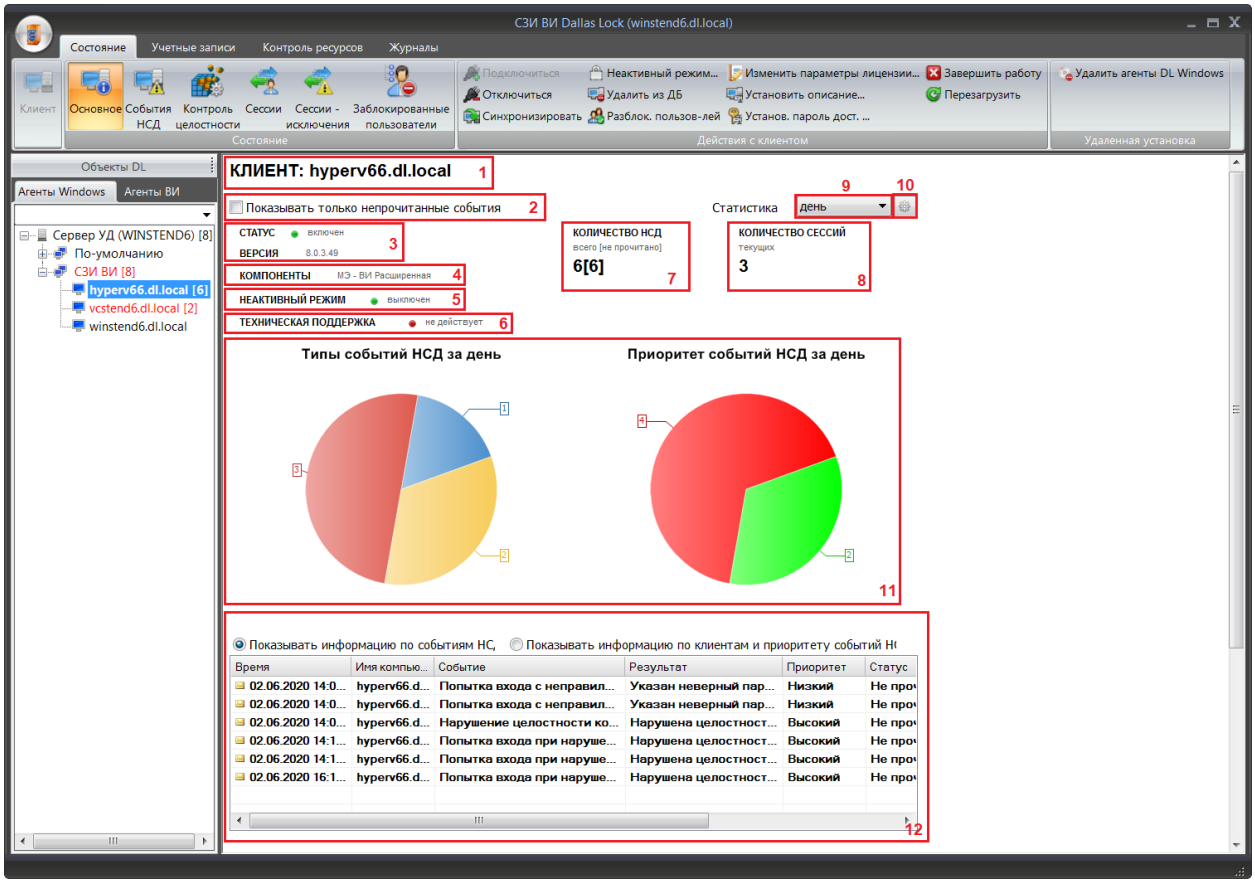


Рис. 76 – Сводная информация по клиенту Windows

Доступны следующие действия с клиентом (некоторые действия доступны только при подключении к клиенту):

- подключиться к клиенту;
- отключиться от клиента;
- провести синхронизацию параметров безопасности клиента Windows по команде администратора (см. п. 3.5 «Синхронизация»);
- включение и настройка неактивного режима (см. п. 3.7 «Неактивный режим»);
- удалить клиента из домена безопасности (при этом компоненты защиты не удаляются с клиента);
- разблокировать пользователей клиента (см. п. 5.1.5.1 «Разблокирование учетных записей клиентов Windows»);
- изменить номер лицензии и код технической поддержки на клиенте (см.п. 11.3 «Настройки лицензирования»);
- установить описание к клиенту. Позволяет установить краткое описание, которое будет добавлено к имени клиента в списке объектов;
- установить пароль доступа для служебного пользователя (учетная запись «secServer») для данного клиента. Используется при невозможности синхронизации клиента с ЦУ СЗИ ВИ. В этом случае, вместе с установкой нового пароля доступа в Консоли ЦУ СЗИ ВИ для клиента, следует изменить и пароль учетной записи «secServer» в оболочке администратора на самом клиенте;

- завершить работу клиента;
- перезагрузить клиент.

Примечание. Для активации кнопок в блоке «Состояние» и блоке «Действия с клиентом» необходимо нажать кнопку «Подключиться», чтобы осуществить оперативное подключение к клиенту.

3.2.2 Дерево «Агенты ВИ»

При выборе в дереве «Агенты ВИ» корневого элемента «Сервер УД» в рабочей области отображается следующая информация (рис. 77)[18]:

1. наименование сервера УД, а также информация о подключении к серверу ЕЦУ;
2. редакция СЗИ ВИ (Стандартная/Расширенная);
3. опция выбора только непрочитанных событий НСД для отображения на круговых диаграммах (8);
4. количество событий НСД (зарегистрированных / не прочитанных);
5. количество лицензий: общие и по каждой платформе виртуализации;
6. блок выборки отображаемых данных по времени («день», «неделя», «месяц», «период»);
7. кнопка вызова настроек приоритетов и оформления круговых диаграмм;
8. круговые диаграммы (события НСД по типу и по приоритету).

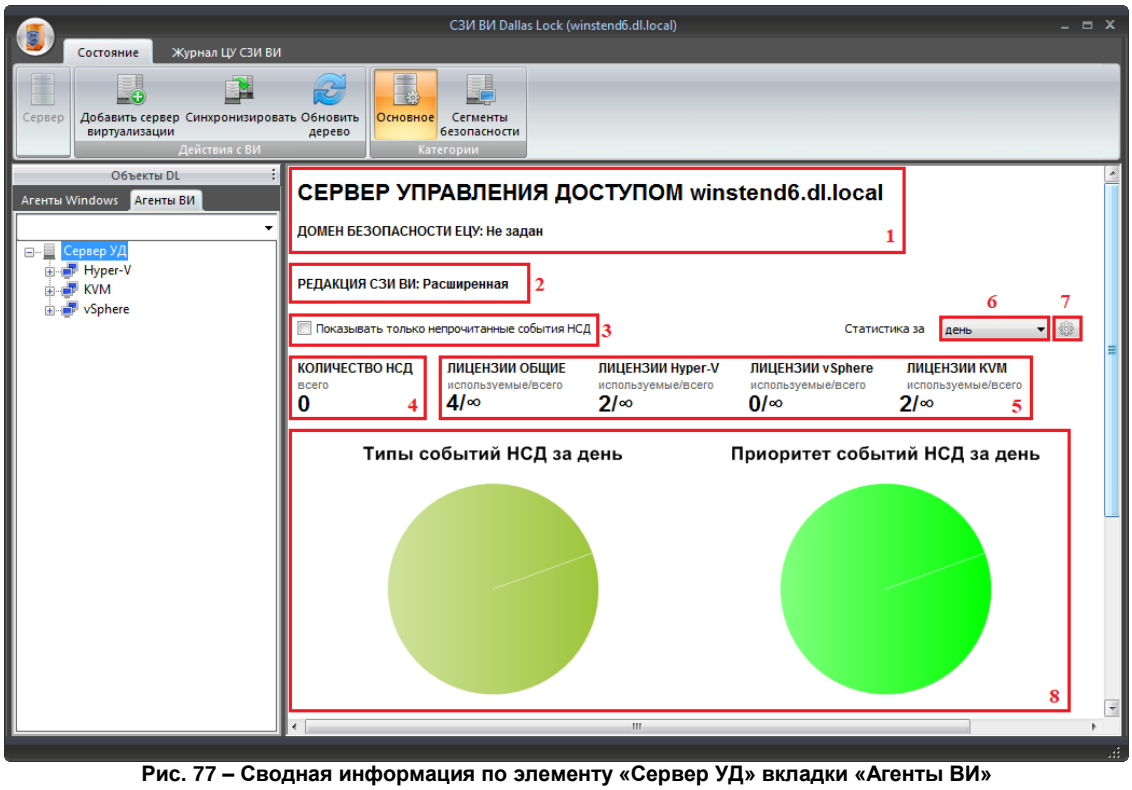


Рис. 77 – Сводная информация по элементу «Сервер УД» вкладки «Агенты ВИ»

При нажатии на кнопку настроек приоритетов и оформления круговых диаграмм (7) откроется окно с настройками отображения типов событий по приоритетам (рис. 78) и по цветам (рис. 79).

[18] В редакции «Стандартная» не отображаются элементы 3, 6, 7, 8.

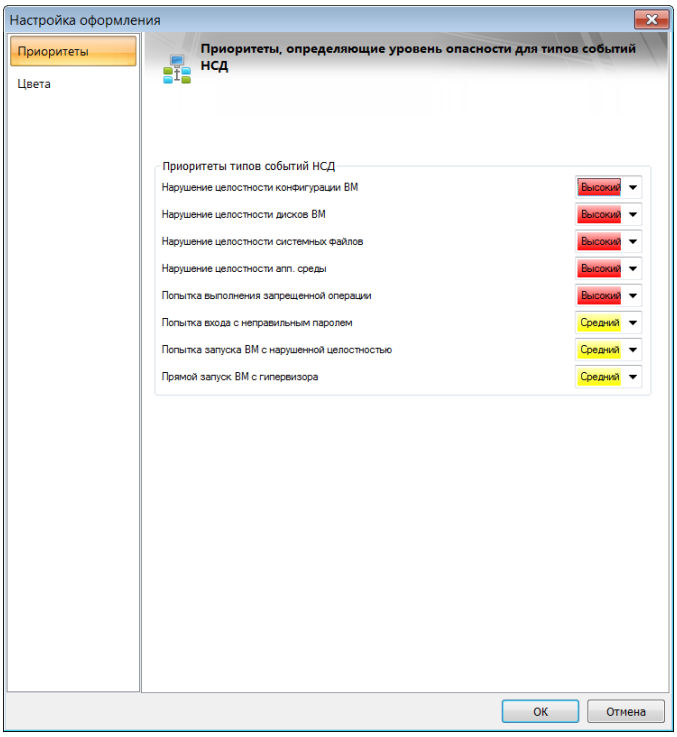


Рис. 78 – Настройка приоритетов типов событий НСД агентов ВИ

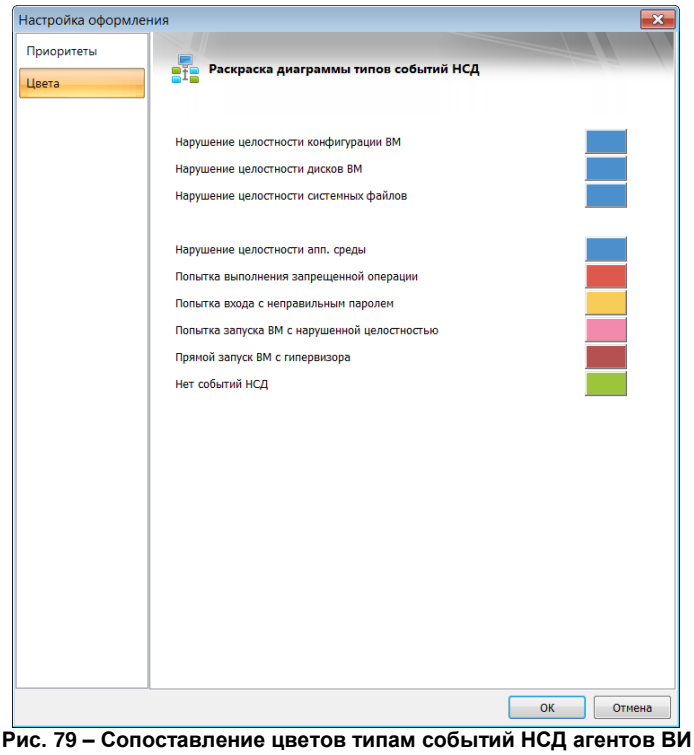


Рис. 79 – Сопоставление цветов типам событий НСД агентов ВИ

Окна отображают перечень типов событий НСД, регистрация которых включена для выбранного элемента дерева – Сервера УД или одной из групп. Для изменения перечня регистрируемых событий см. п. 3.6 «Сигнализация об НСД».

3.2.2.1 Информационная панель групп ВИ

Группы элементов «vSphere», «Hyper-V» и «KVM» единообразно настраиваются и отображают информацию о себе. При выборе группы в дереве «Агенты ВИ» состояние объектов группы отображается в рабочей области (рис. 80)[19].

[19] Круговые диаграммы (события НСД по типу и по приоритету) доступны только в редакции «Расширенная».

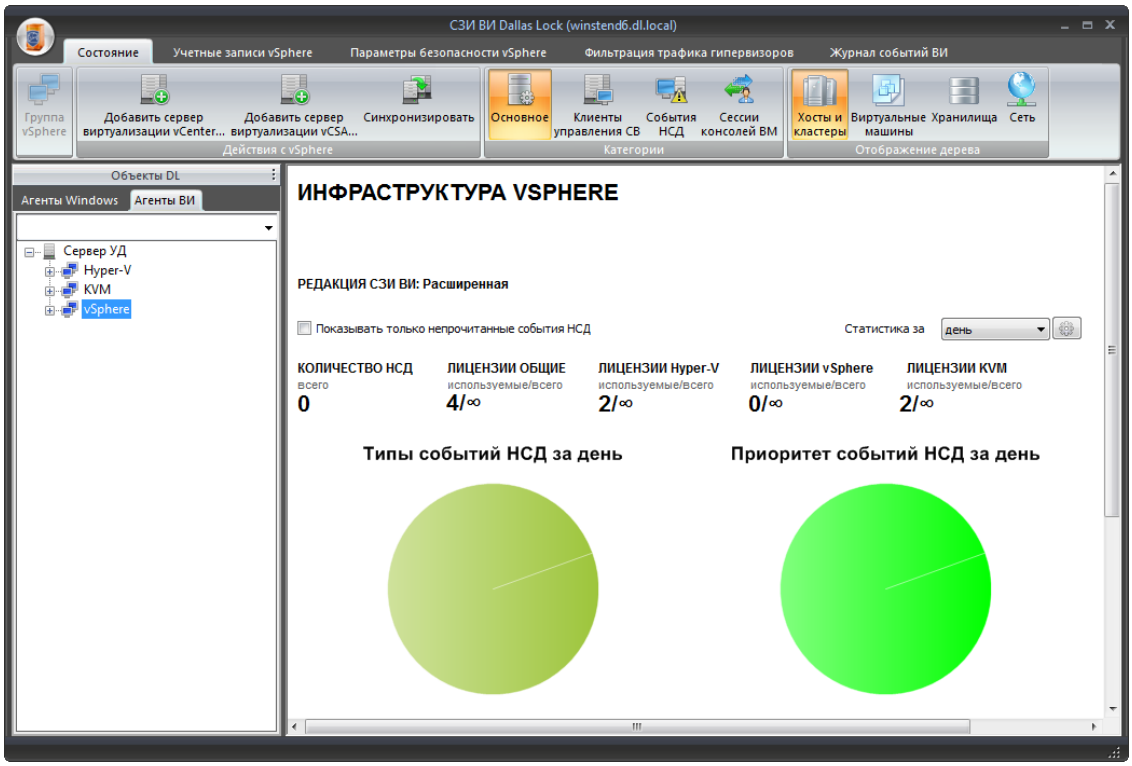


Рис. 80 – Сводная информация по группе vSphere

Доступны следующие действия с группами:

- добавление сервера виртуализации;
- синхронизация параметров безопасности всех объектов группы по команде администратора (см. п. 3.5 «Синхронизация»);

Для группы объектов ВИ «vSphere» есть возможность изменить отображение дерева объектов. Режимы отображения повторяют штатные режимы отображения VMware.

Доступны следующие режимы отображения дерева ВИ группы vSphere:

- Хосты и кластеры – наиболее полный режим отображения.
- Виртуальные машины – отображаются виртуальные машины и их вышестоящая иерархия.
- Хранилища – datastores и пр.
- Сеть – объекты сети (виртуальные коммутаторы и пр.).

По умолчанию дерево отображается в режиме «Хосты и кластеры».

3.2.2.2 Информационная панель СВ vSphere

Просмотр основных параметров СВ vCenter происходит на уровне Сервера виртуализации в категории «Состояние» → «Основное».

Данная категорию содержит элементы управления СВ, а также отображает статус учетных данных, статус и версию агента DL vCenter/vCSA, версию vCenter, количество хостов (активные/всего), количество ВМ (включено/всего) и список последних событий журнала СВ (рис. 81).

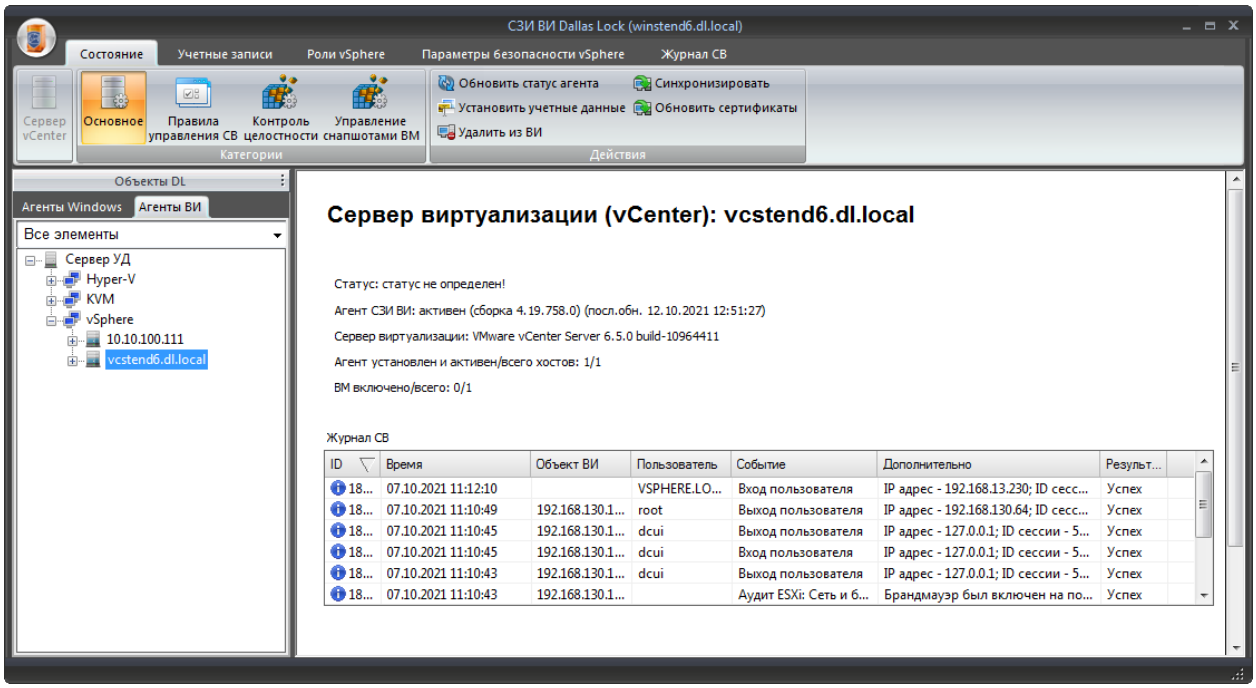


Рис. 81 – Рабочая область СВ vCenter

Доступны следующие действия с Сервером виртуализации:

- обновление статуса агента DL;
- установка учетных данных для подключения к Серверу виртуализации;
- удаление (вывод) Сервера виртуализации из ВИ;
- синхронизация параметров безопасности Сервера виртуализации с ЦУ СЗИ ВИ (см. п. 3.5 «Синхронизация»);
- обновление сертификатов Сервера виртуализации;
- инициализировать.

3.2.2.3 Информационная панель СВ Hyper-V

Просмотр основных параметров СВ Hyper-V происходит на уровне Сервера виртуализации в категории «Состояние» → «Основное».

Данная категорию содержит элементы управления СВ, а также отображает статус учетных данных, статус и версию агента DL Hyper-V, версию ОС, количество ВМ (включено/всего) и список последних событий журнала СВ (рис. 82).

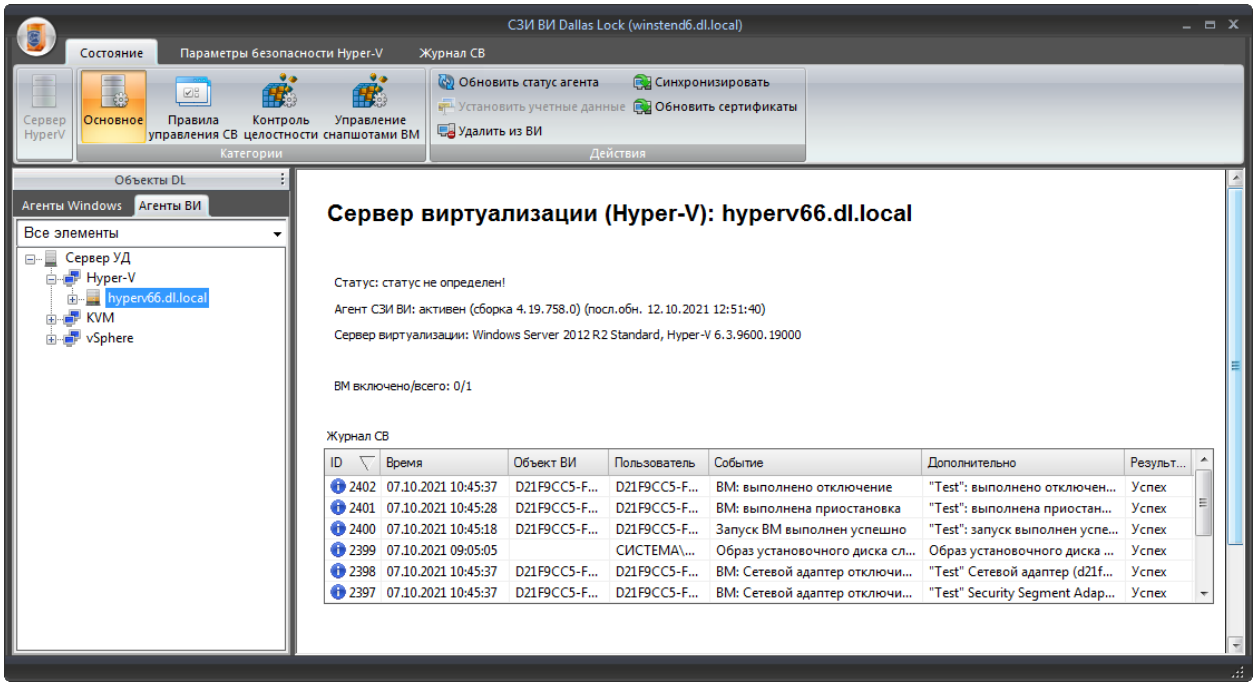


Рис. 82 – Рабочая область СВ Hyper-V

Доступны следующие действия с Сервером виртуализации:

- обновление статуса агента DL;
- установка учетных данных для подключения к Серверу виртуализации;
- удаление (вывод) Сервера виртуализации из ВИ;
- синхронизация параметров безопасности Сервера виртуализации с ЦУ СЗИ ВИ (см. п. 3.5 «Синхронизация»);
- обновление сертификатов Сервера виртуализации.

3.2.2.4 Информационная панель гипервизора ESXi

Просмотр основных параметров гипервизора происходит на уровне гипервизора ESXi в категории «Состояние» → «Основное».

Данная категорию содержит элементы управления гипервизора, а также отображает статус учетных данных, статус и версию агента DL ESXi, версию ESXi, количество процессоров на гипервизоре и количество ВМ (включено/всего) (рис. 83).

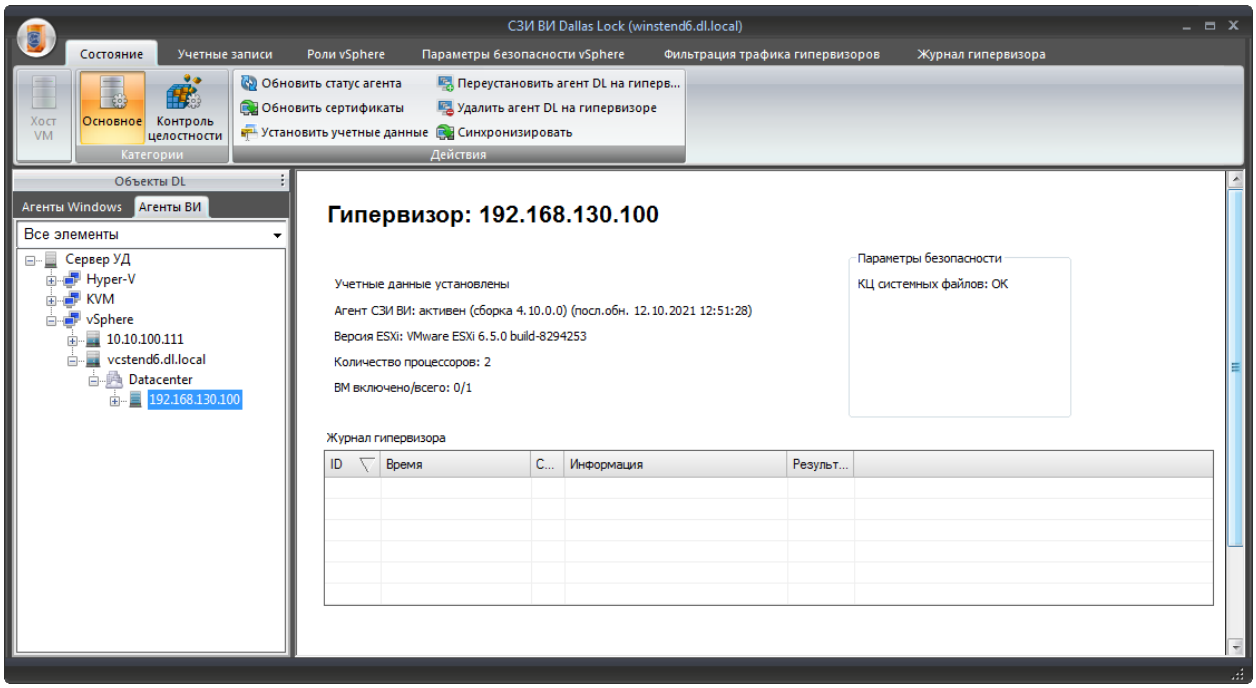


Рис. 83 – Рабочая область гипервизора ESXi

Доступны следующие действия с гипервизором:

- обновление статуса агента DL ESXi;
- обновление сертификатов гипервизора;
- установка учетных данных для подключения к ESXi;
- установка (переустановка) агента DL ESXi на гипервизоре;
- удаление агента DL ESXi на гипервизоре;
- синхронизация параметров безопасности с ЦУ СЗИ ВИ (см. п. 3.5 «Синхронизация»).

3.2.2.5 Информационная панель гипервизора KVM

Просмотр основных параметров гипервизора происходит на уровне гипервизора KVM в категории «Состояние» → «Основное».

Данная категорию содержит элементы управления гипервизора, а также отображает статус учетных данных, статус и версию агента DL ESXi, версию ESXi, количество процессоров на гипервизоре (рис. 84).

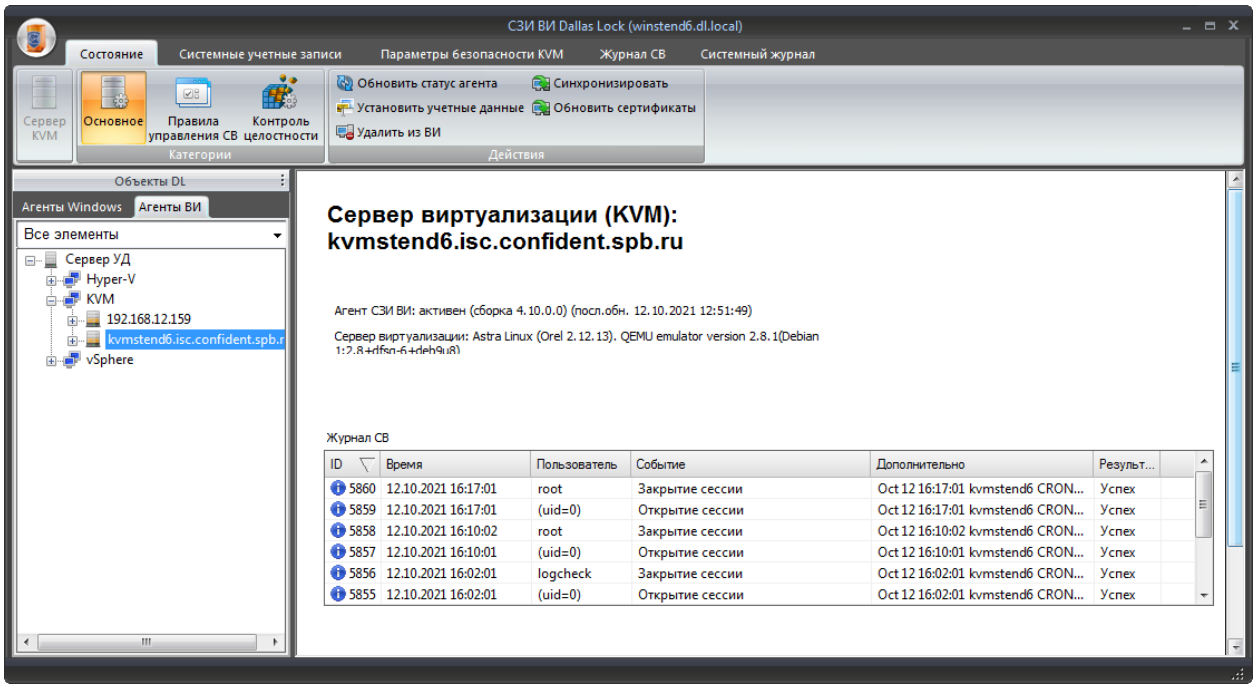


Рис. 84 – Рабочая область гипервизора KVM

Доступны следующие действия с гипервизором:

- обновление статуса агента DL KVM;
- установка пароля для учетной записи администратора;
- удаление агента DL KVM на гипервизоре;
- синхронизация параметров безопасности с ЦУ СЗИ ВИ (см. п. 3.5 «Синхронизация»);
- обновление сертификатов гипервизора.

3.2.2.6 Информационная панель СВ oVirt/zVirt/HOSTVM/РЕД Вирт

Просмотр основных параметров СВ oVirt/zVirt/HOSTVM/РЕД Вирт происходит на уровне Сервера виртуализации в категории «Состояние» → «Основное».
Данная категорию содержит элементы управления СВ, а также отображает статус и версию агента DL Engine и список последних событий журнала СВ (рис. 85).

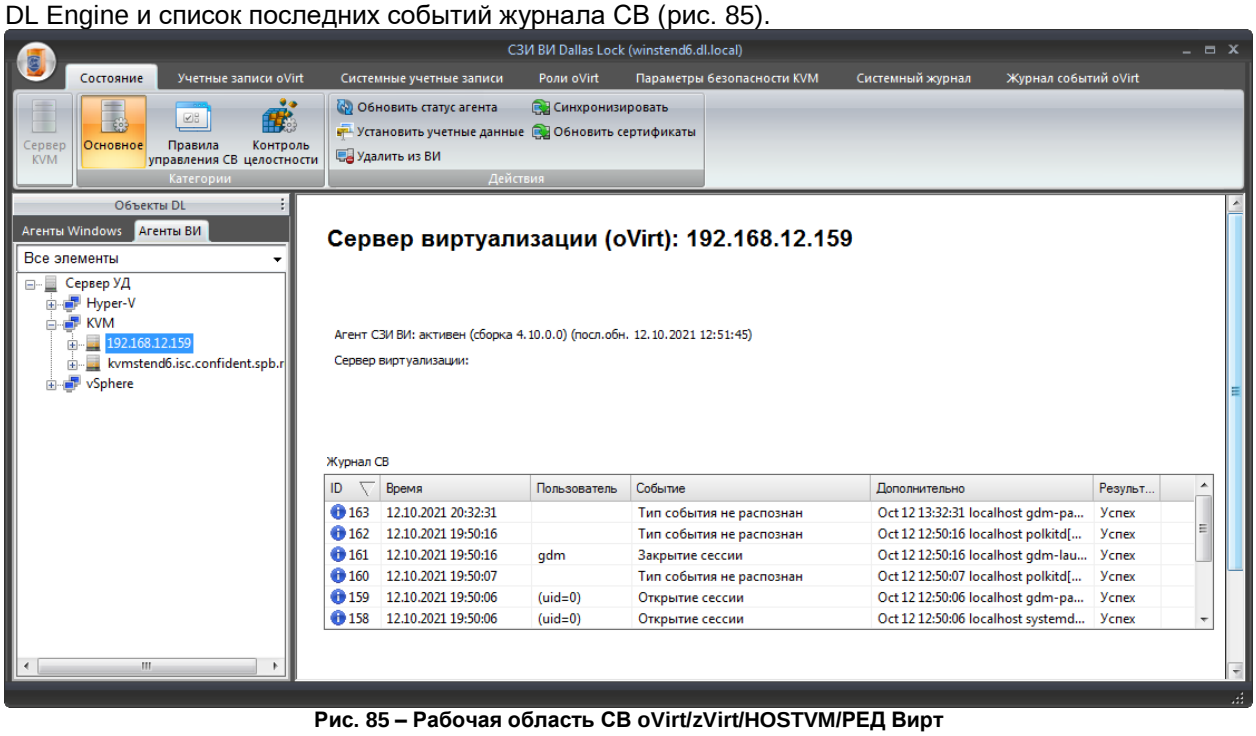


Рис. 85 – Рабочая область СВ oVirt/zVirt/HOSTVM/РЕД Вирт

Доступны следующие действия с СВ:

- обновление статуса агента DL Engine;
- установка пароля для учетной записи администратора;

- удаление агента DL Engine на СВ;
- синхронизация параметров безопасности с ЦУ СЗИ ВИ (см. п. 3.5 «Синхронизация»);
- обновление сертификатов СВ.

3.2.2.7 Информационная панель гипервизора oVirt/zVirt/HOSTVM/РЕД Вирт

Просмотр основных параметров гипервизора oVirt/zVirt/HOSTVM/РЕД Вирт происходит на уровне гипервизора в категории «Состояние» → «Основное».
Данная категорию содержит элементы управления гипервизора, а также отображает статус учетных данных, статус и версию агента DL Host (рис. 86).

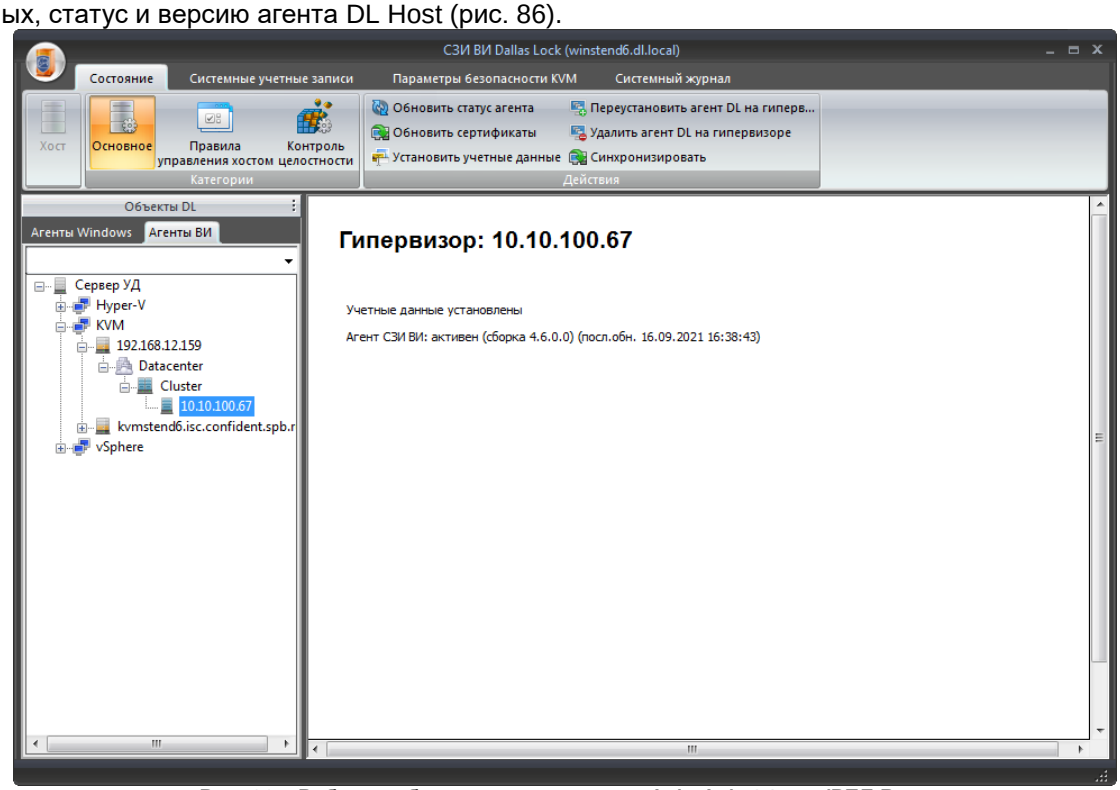


Рис. 86 – Рабочая область гипервизора oVirt/zVirt/HOSTVM/РЕД Вирт

Доступны следующие действия с гипервизором:

- обновление статуса агента DL Host;
- обновление сертификатов гипервизора;
- установка учетных данных для подключения к гипервизору oVirt/zVirt/HOSTVM/РЕД Вирт;
- установка (переустановка) агента DL Host на гипервизоре;
- удаление агента DL Host на гипервизоре;
- синхронизация параметров безопасности с ЦУ СЗИ ВИ (см. п. 3.5 «Синхронизация»).

3.3 Основные параметры

Настройка основных параметров функционирования СЗИ ВИ осуществляется выбором пункта «Параметры сервера УД» в дополнительном меню Консоли (рис. 87). В открывшемся окне путем выбора соответствующих вкладок в меню слева можно задать настройки для агентов Windows, ядра СЗИ ВИ и групп объектов ВИ (рис. 88).

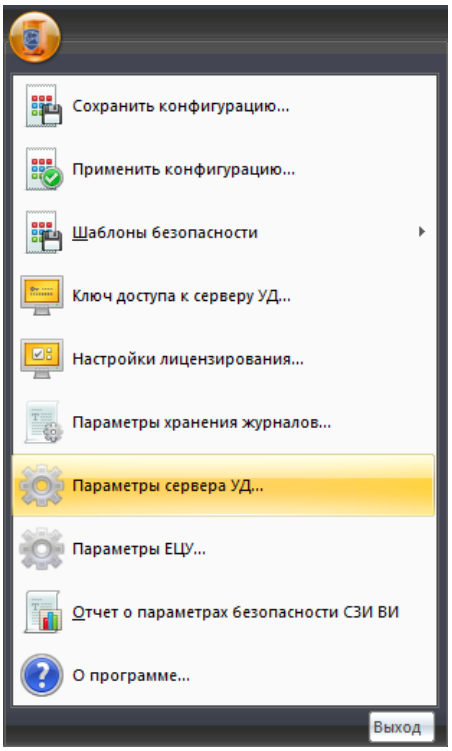


Рис. 87 – Дополнительное меню Консоли СЗИ ВИ

3.3.1 Основные параметры работы агентов Windows

Для настройки параметров работы агентов Windows необходимо выбрать вкладку «WINDOWS» в меню слева.

Во фрейме справа отобразится перечень доступных настроек:

- опция «Синхронизация системного времени клиентов Windows»;
- частота периодической синхронизации;
- расписание синхронизации;
- частота периодического сбора журналов;
- расписание сбора журналов;
- настройка оповещения о событиях на клиентах (см. п. 3.6 «Сигнализация об НСД»).

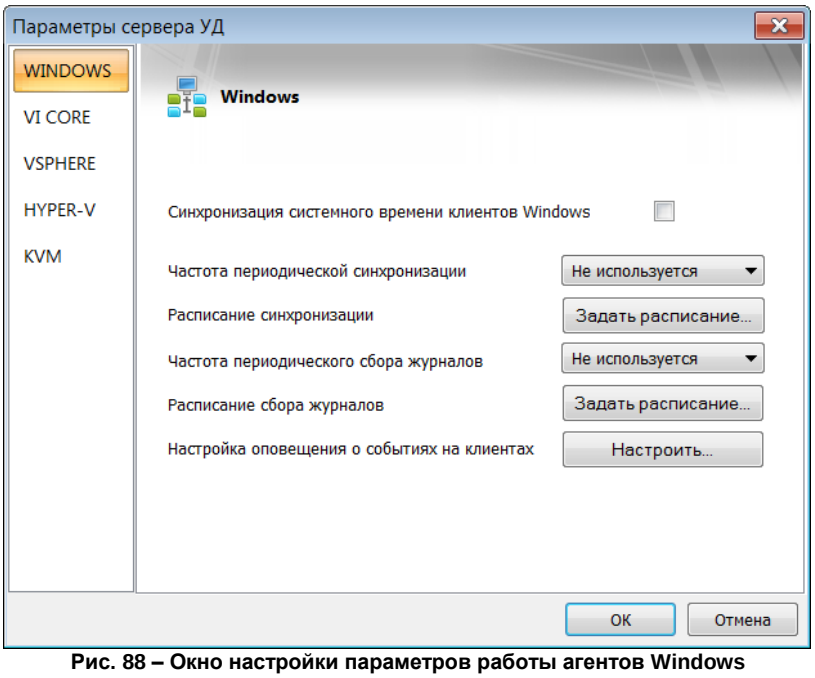


Рис. 88 – Окно настройки параметров работы агентов Windows

После внесения изменений необходимо нажать кнопку «OK».

3.3.2 Основные параметры работы ядра СЗИ ВИ

Для настройки работы ядра СЗИ ВИ необходимо выбрать пункт «VI CORE» в меню слева. Во фрейме справа отобразится перечень доступных настроек:

- частота проверки КЦ системных файлов;
- расписание проверки КЦ системных файлов;
- частота периодической синхронизации СВ;
- расписание синхронизации СВ;
- частота периодического сбора журналов СВ;
- расписание сбора журналов СВ;
- синхронизация времени клиентов (настройка NTP);
- настройка оповещения о событиях в ВИ (см. п. 3.6 «Сигнализация об НСД»);
- максимальное кол-во доверенных клиентов (см. п. 6.3.2 «Клиенты управления СВ»).

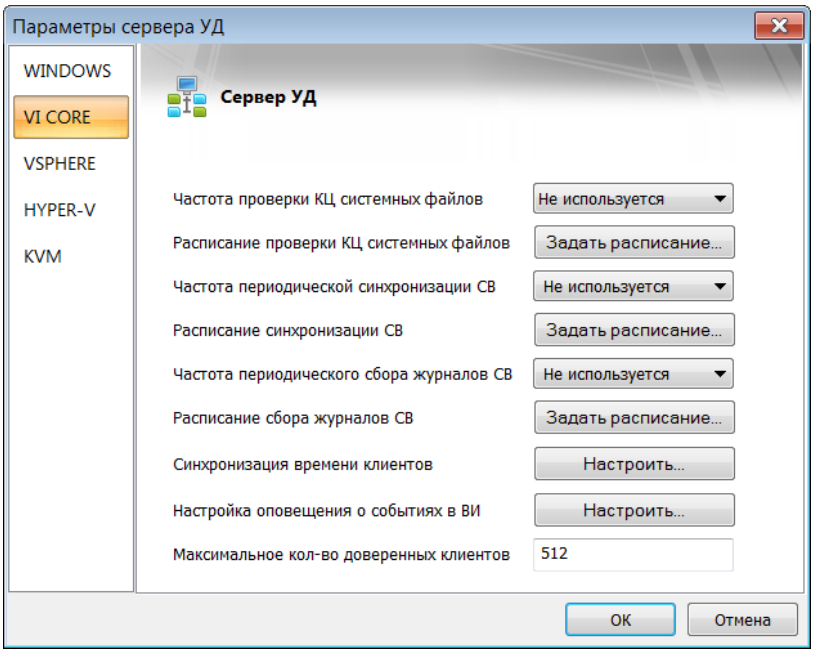


Рис. 89 – Окно настройки параметров работы ядра СЗИ ВИ

После внесения изменений необходимо нажать кнопку «ОК».

3.3.3 Основные параметры группы СВ vSphere

В окне настройки параметров сервера УД для группы vSphere доступны следующие настраиваемые параметры:

- частота периодической проверки КЦ системных файлов (необходимо выбрать период времени);
- расписание проверки КЦ системных файлов;
- частота периодической синхронизации СВ;
- расписание синхронизации СВ;
- частота периодического сбора журналов СВ;
- расписание сбора журналов СВ.

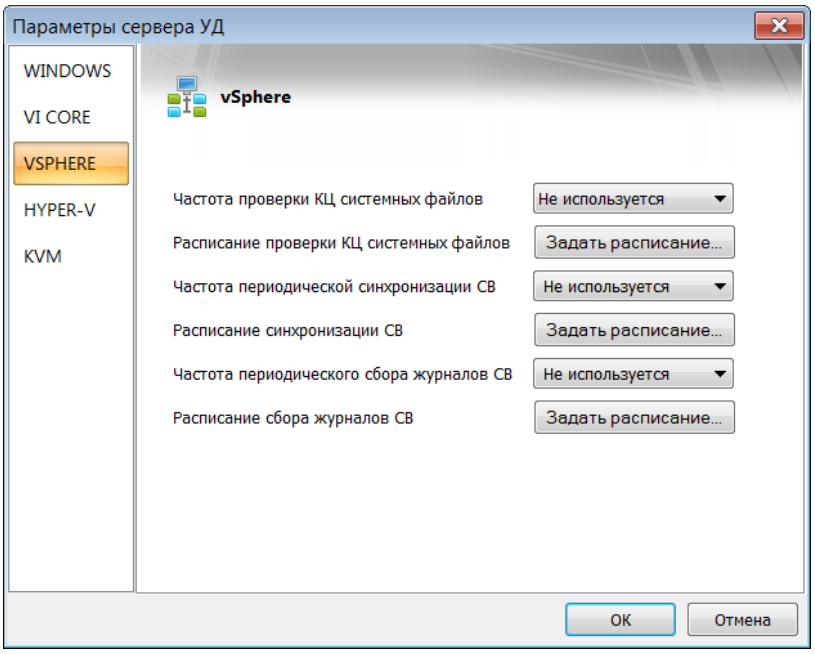


Рис. 90 – Окно настройки параметров группы vSphere

Применение внесенных изменений происходит по нажатию кнопки «ОК».

3.3.4 Основные параметры группы СВ Hyper-V

В окне настройки параметров сервера УД для группы Hyper-V доступны следующие настраиваемые параметры:

- частота периодической синхронизации СВ;
- расписание синхронизации СВ;
- частота периодического сбора журналов СВ;
- расписание сбора журналов СВ.

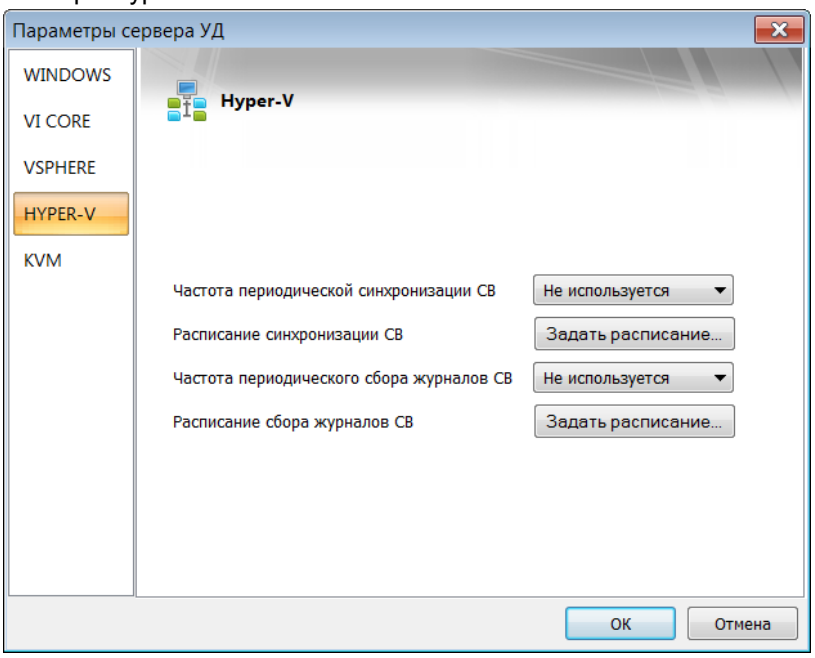


Рис. 91 – Окно настройки параметров группы Hyper-V

Применение внесенных изменений происходит по нажатию кнопки «ОК».

3.3.5 Основные параметры группы KVM

В окне настройки параметров сервера УД для группы KVM доступны следующие настраиваемые параметры:

- частота периодической проверки КЦ системных файлов (необходимо выбрать период времени);

- расписание проверки КЦ системных файлов;
- частота периодической синхронизации СВ;
- расписание синхронизации СВ.

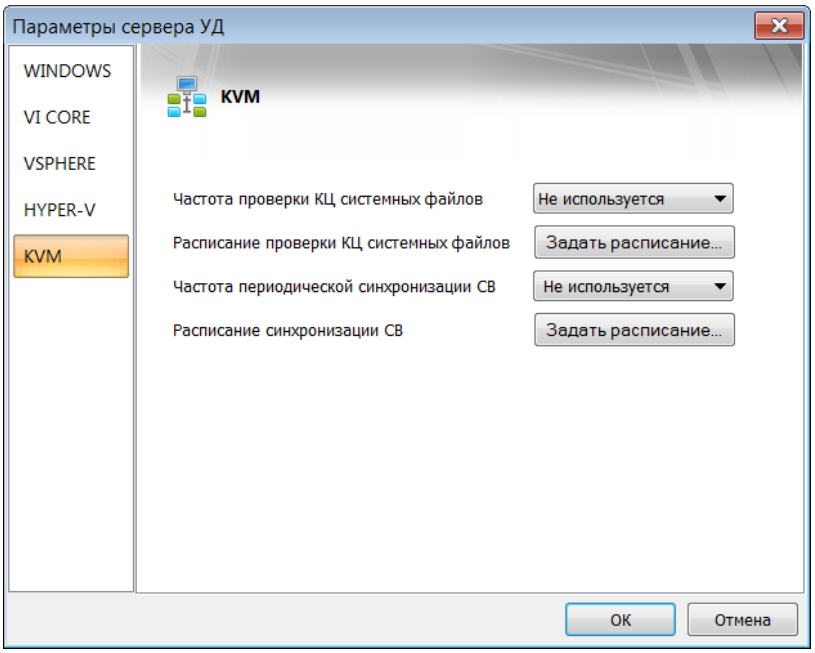


Рис. 92 – Окно настройки параметров группы KVM

Применение внесенных изменений происходит по нажатию кнопки «OK».

3.4 Ролевая модель учетных записей СУД

Контроль доступа к ЦУ СЗИ ВИ осуществляется средствами ролевой модели разграничения доступа. Для работы с ролями необходимо на уровне Сервера УД перейти в категорию «Администрирование на СУД» → «Роли» (рис. 93).

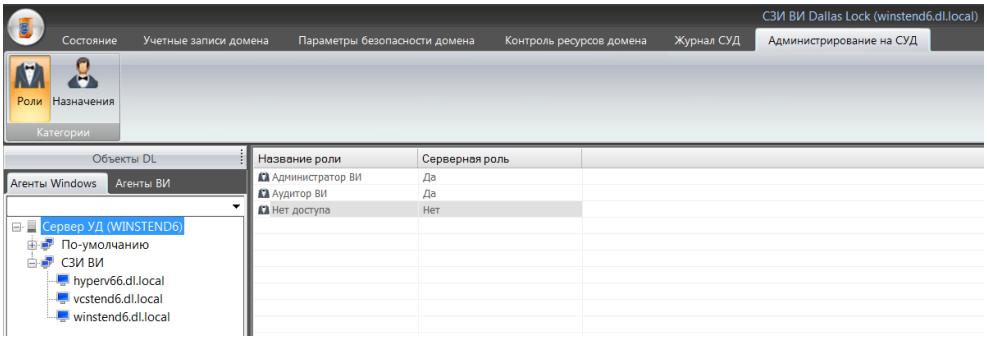


Рис. 93 – Предустановленные роли

Роль представляет собой совокупность привилегий – полномочий по выполнению действий в части администрирования СУД и домена безопасности. Для удобства привилегии группируются в несколько категорий в зависимости от области применения.

Различным учетным записям (или группам пользователей) домена безопасности имеется возможность присвоить определенную роль. Список назначенных ролей можно посмотреть, перейдя в категорию «Назначения».

Рабочая область категории «Роли» состоит из двух разделов: «Название роли» и «Серверная роль».

Если роль является серверной, то ее можно назначить только для СУД, и для нее все привилегии из раздела «Управление СУД» являются неактивными.

Для доменной роли осуществляется автоматическое наследование назначения на более низкоуровневых узлах.

В СУД существуют три предустановленные роли, которые невозможно отредактировать или удалить:

- Администратор ВИ (предполагает полный доступ к работе с Консолью ЦУ СЗИ ВИ и веб-консолью СЗИ ВИ (подробнее работа с веб-консолью описана в разделе 4 «ОПИСАНИЕ СРЕДСТВ АУДИТА»));

- Аудитор ВИ (предполагает работу только с подсистемой аудита в Консоли ЦУ СЗИ ВИ и веб-консоли СЗИ ВИ (подробнее работа с журналами описана в разделе 9 «ПОДСИСТЕМА АУДИТА»), работа с веб-консолью описана в разделе 4 «ОПИСАНИЕ СРЕДСТВ АУДИТА»);
- Нет доступа.

3.4.1 Создание, изменение и удаление назначений ролей

Назначение предустановленных ролей пользователям или группам пользователей происходит в категории «Назначения» (рис. 94).

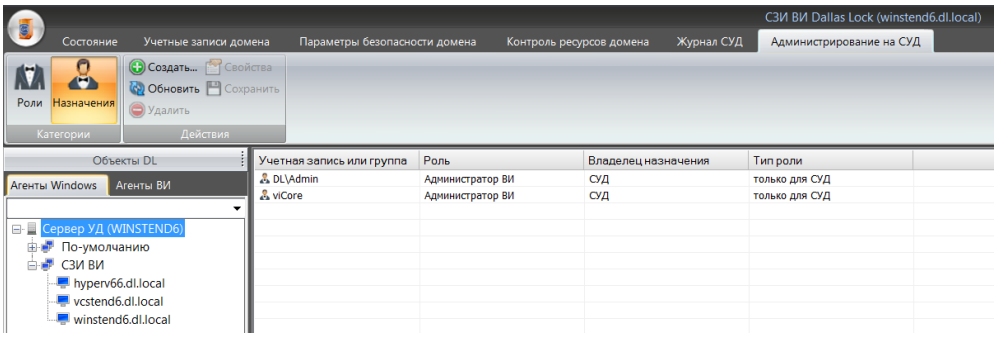


Рис. 94 – Назначение предустановленных ролей

Для назначения одной из предустановленных ролей для пользователя или группы, необходимо нажать на кнопку «Создать» в блоке «Действия». В появившемся окне указать место размещения предварительно созданной учетной записи пользователя или группы пользователей, которым необходимо назначить роль, левой кнопкой мыши выбрать одну или несколько учетных записей пользователей или групп, из раскрывающегося списка выбрать одну из трех ролей, которую необходимо назначить и нажать кнопку «ОК» (рис. 95).

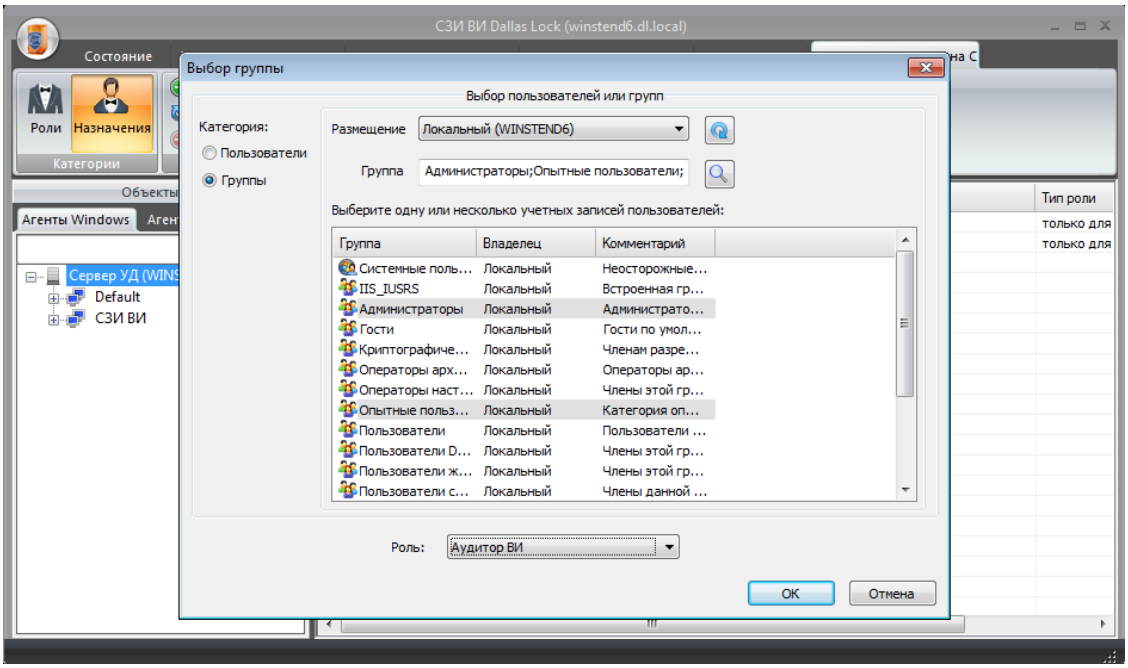


Рис. 95 – Администрирование на СУД. Назначение роли

Затем необходимо нажать кнопку «Сохранить» в панели действий и в списке учетных записей и групп отобразится учетная запись или группа с назначенной ролью.

Примечание. Для администрирования ЦУ СЗИ ВИ доменным пользователем его учетная запись должна быть зарегистрирована в системе защиты отдельно, а не с помощью маски «*/*» (подробнее в п. 5.1.2.2 «Регистрация доменных учетных записей»).

После входа в Консоль под учетной записью пользователя с правами только на просмотр параметры безопасности будут отображены, но не будет возможности их редактировать, производить настройки и действия; кнопки, отвечающие за настройки, будут недоступны.

Смена роли для учетной записи или группы осуществляется при помощи выделения ее в таблице и нажатия кнопки «Свойства» в блоке «Действия». При этом открывается диалоговое окно с выпадающим списком для выбора назначаемой роли (рис. 96).

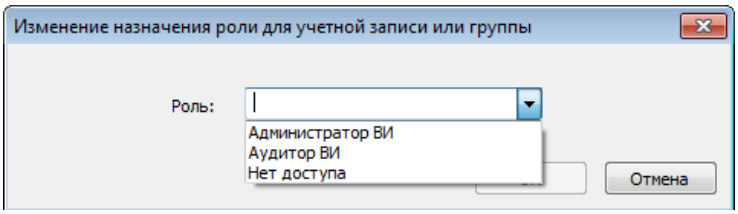


Рис. 96 – Смена роли для учетной записи

Примечание. При назначении роли для учетной записи или группы, для которых назначение уже было создано, происходит переназначение данной роли.

Для удаления назначения необходимо выделить удаляемую роль, на панели сверху нажать кнопку «Удалить» в блоке «Действия» и подтвердить действие в появившемся диалогом окне (рис. 97).

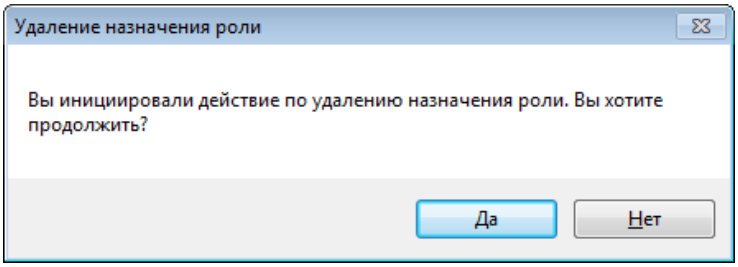


Рис. 97– Удаление назначения роли для учетной записи или группы

После внесения всех необходимых изменений в таблицу, следует выполнить сохранение путем нажатия кнопки «Сохранить» в блоке «Действия».

3.5 Синхронизация

Синхронизация – это ключевое понятие в концепции ЦУ СЗИ ВИ. Под синхронизацией понимается процесс проверки соответствия настройки объектов ВИ с внутренней базой данных ЦУ СЗИ ВИ, являющейся эталонной настройкой ВИ. При обнаружении несоответствия к настройкам объектов ВИ применяются эталонные настройки ЦУ СЗИ ВИ.

Все настройки параметров объектов ВИ, производимые через Консоль ЦУ СЗИ ВИ, считаются эталонными. Любые изменения параметров (умышленные или злоумышленные), происходящие в обход СЗИ ВИ, считаются не действительными и при синхронизации настраиваются согласно записям ЦУ СЗИ ВИ. Если параметры оставались без изменения (например, список пользователей), синхронизация этих параметров не происходит. Факты и результаты синхронизации отображаются в журнале ЦУ СЗИ ВИ.

Синхронизацию по команде администратора возможно произвести для определенного сервера виртуализации или всей ВИ. Для этого необходимо выбрать уровень vSphere, Hyper-V, KVM, CB или гипервизор, открыть вкладку «Состояние» или вызвать контекстное меню и нажать кнопку «Синхронизировать».

Также в окне настройки параметров сервера УД можно задать частоту периодической синхронизации, расписание синхронизации и настройки сетевой службы точного времени.

Частота периодической синхронизации
Данный параметр позволяет производить автоматическую синхронизацию через указанный промежуток времени: от 1 минуты до 24 часов. Для отключения необходимо выбрать значение «Не используется».
Расписание синхронизации
Данный параметр позволяет настроить автоматический сбор журналов по гибкому расписанию. В окне настройки расписания необходимо включить контроль, поставив флаг в поле «Использовать расписание», и составить расписание.
Синхронизация времени клиентов
Данный параметр позволяет задать список NTP-серверов для синхронизации времени между сервером УД и агентами СЗИ ВИ

3.6 Сигнализация об НСД

Ситуации несанкционированного доступа на Объекты ВИ отслеживаются и сопровождаются

сигнализацией на Сервер УД. Сообщения о событиях НСД заносятся в журнал Сервера УД. При попытке НСД на ПК с установленной СЗИ ВИ воспроизводится звуковой сигнал, выводится соответствующее всплывающее сообщение в области уведомлений Windows (рис. 98).

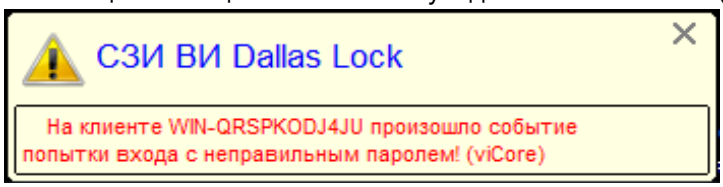


Рис. 98 – Сигнализация об НСД в области уведомлений

Также количество событий НСД отображается в квадратных скобках рядом с элементами дерева на вкладке «Агенты Windows» (рис. 99).

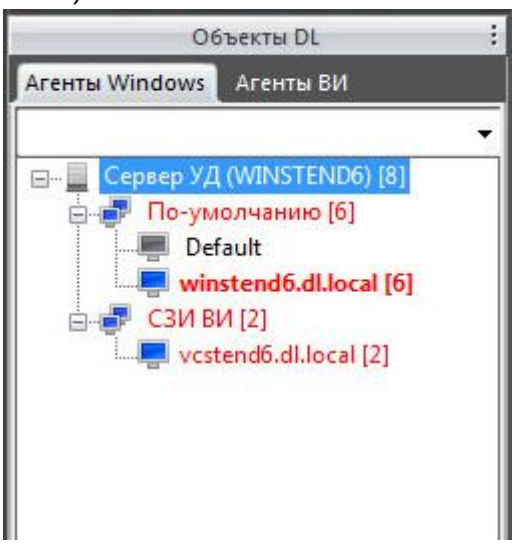


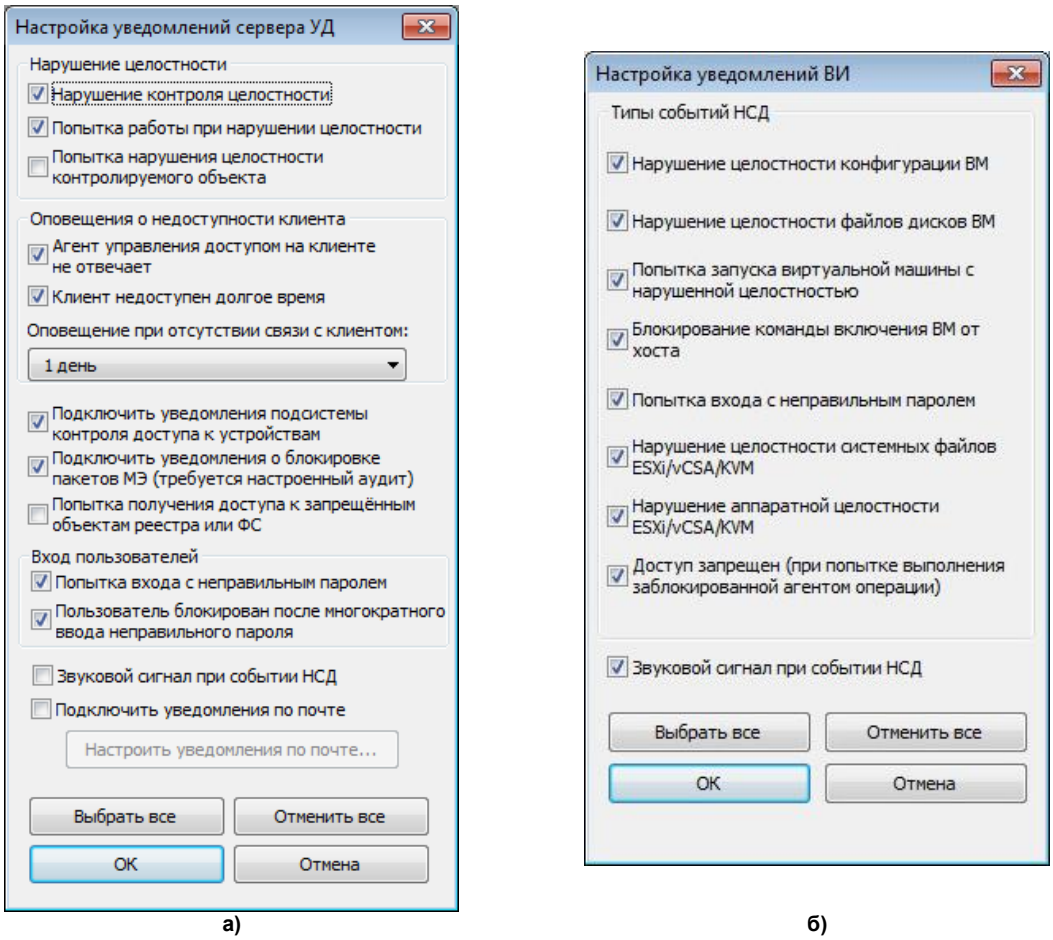
Рис. 99 – Сигнализация об НСД в дереве «Агенты Windows»

События, зафиксированные на объектах нижнего уровня, суммируются на объектах более высокого уровня, вплоть до объекта «Сервер УД», который может отображать все события НСД всех объектов структуры дерева СЗИ ВИ.

При прочтении одного события НСД в списке событий НСД на том или ином уровне, количество событий НСД, отображаемое на этом уровне, уменьшается на единицу и все суммируемые события НСД на более высоких уровнях так же уменьшается на единицу. При прочтении большего количества событий НСД, отображаемые в дереве непрочитанные события уменьшатся на количество прочитанных событий НСД.

Для того чтобы произвести настройку уведомлений, получаемых от соответствующих агентов (Windows или ВИ), необходимо:

1. В дополнительном меню выбрать пункт «Параметры сервера УД», откроется окно «Параметры сервера УД».
2. В меню слева выбрать необходимую группу («WINDOWS» или «VI CORE»), отобразится соответствующий группе перечень настроек. Нажать кнопку «Настроить» для параметра «Настройка оповещения о событиях на клиентах» в случае группы «WINDOWS» или «Настройка оповещения о событиях в ВИ» в случае группы «VI CORE».
3. В появившемся окне установить флаги для необходимых событий (рис. 100).



а) **б)**

Рис. 100 – Настройка уведомлений событий агентов Windows (а) и виртуальной инфраструктуры (б)

Сигнализация при нарушении целостности происходит при ее проверке. Частота периодической проверки КЦ системных файлов гипервизора редактируется только для всех гипервизоров (см. п. 3.3.3 «Основные параметры группы СВ vSphere»). Частота периодической проверки КЦ для ВМ редактируется при настройке КЦ для ВМ (см. п. 7.2 «Настройка контроля целостности ВМ»).

Примечание. При многократной проверке объекта ВИ с нарушенной целостностью сигнализация происходит только при первом обнаружении нарушения. Повторная сигнализация о том же нарушении не произойдет!

Просмотр событий сигнализации доступен как для клиентов Windows, так и для групп ВИ:

1. Для просмотра событий сигнализации на клиентах Windows необходимо в дереве «Агенты Windows» на уровне клиента открыть категорию «Состояние» → «События НСД» (рис. 101). Имя клиента, подвергшегося попытке НСД, в дереве отмечается красным цветом.

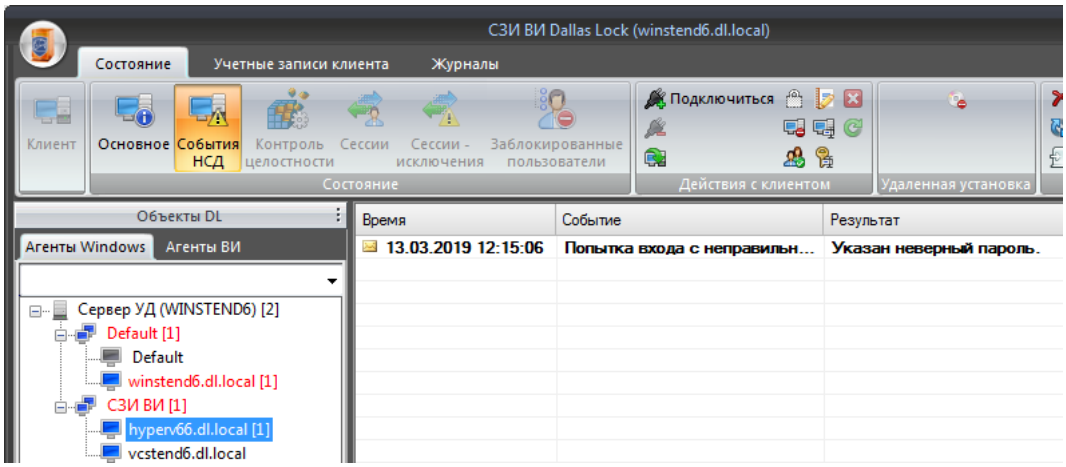


Рис. 101 – Журнал событий сигнализации об НСД клиента Windows

2. Для просмотра событий сигнализации на клиентах ВИ необходимо в дереве «Агенты ВИ» на уровне группы Hyper-V/KVM/vSphere открыть категорию «Состояние» → «События НСД» (рис. 102). Имя клиента, подвергшегося попытке НСД, в дереве отмечается красным цветом.

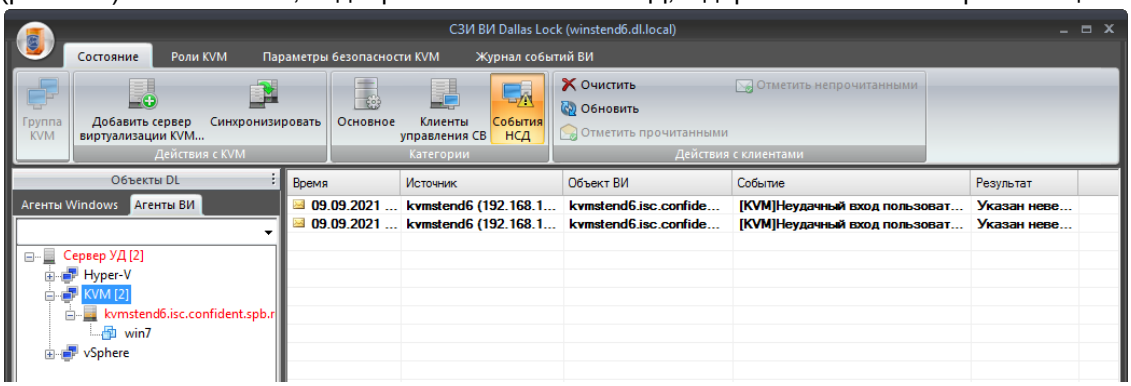


Рис. 102 – Журнал событий сигнализации об НСД на примере KVM

С помощью панели действий и контекстного меню для списка событий НСД возможно отметить все записи прочитанными или непрочитанными, обновить и очистить список, загрузить сообщения о событиях НСД из текущего журнала[20]. Двойной клик по событию откроет запись в отдельном окне, в списке данное событие будет помечено как прочитанное.

3.7 Неактивный режим

В СЗИ ВИ реализован особый механизм контроля доступа к ресурсам – неактивный режим. Неактивный режим – режим, в котором возможно полное или частичное отключение подсистем СЗИ ВИ. Режим используется для диагностики нежелательного вмешательства СЗИ ВИ в работу ОС и сторонних приложений. Для включения/настройки режима, пользователю нужно право на деактивацию СЗИ ВИ.

Неактивный режим возможно настроить для Сервера УД, либо для отдельной группы клиентов Windows.

Для этого необходимо во вкладке «Агенты Windows» на уровне Сервера УД или группы клиентов во вкладке «Состояние» при активной категории «Основное» нажать кнопку «Неактивный режим». В появившемся окне (рис. 103) установить флаг в поле «Неактивный режим» и выбрать параметры СЗИ ВИ, которые необходимо отключить. Нажать кнопку «ОК».

[20] Загрузка сообщений о событиях НСД из текущего журнала доступна только для клиентов Windows.

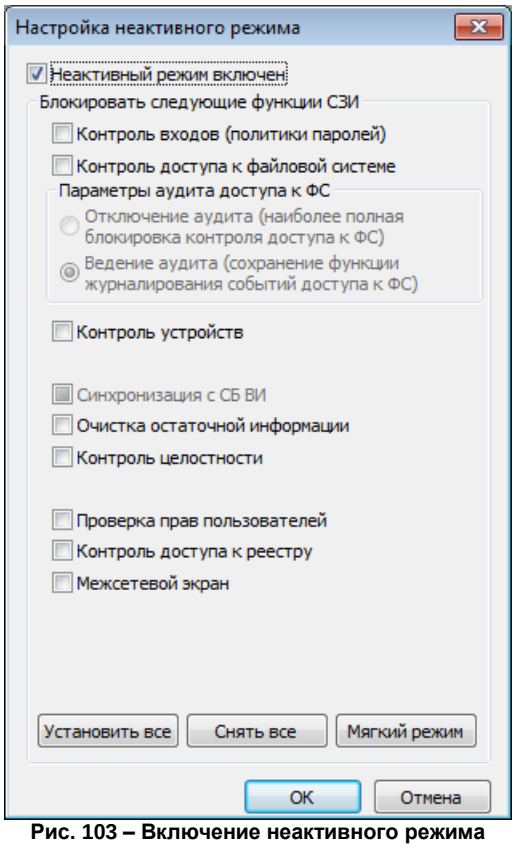


Рис. 103 – Включение неактивного режима

После включения или отключения неактивного режима необходимо проводить синхронизацию настроек. Для этого в категории «Действия с доменом» необходимо нажать кнопку «Синхронизировать».

На уровне группы для включения неактивного режима производятся действия аналогичные действиям на уровне Сервера УД.

Внимание! Включение неактивного режима достаточно рискованно для обеспечения информационной безопасности, так как любой пользователь получает доступ к любому объекту ФС. Поэтому важно отключать эти режимы, когда в них нет необходимости.

Для напоминания о том, что включены данные режимы, при входе пользователя после загрузки ОС в области уведомлений Windows будет появляться всплывающее предупреждение (рис. 104).

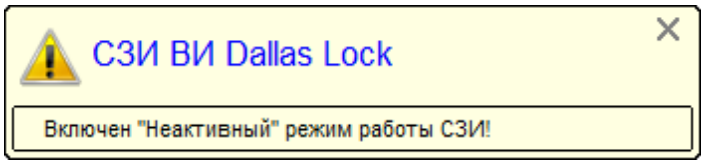


Рис. 104 – Предупреждение о включенном неактивном режиме

Для включения/выключения неактивного режима пользователь должен быть наделен правами на деактивацию системы защиты (вкладка «Параметры безопасности домена» → «Права пользователей» → параметр «Деактивация системы защиты»).

3.7.1 Мягкий режим

Включение и настройка мягкого режима производится в окне настройки неактивного режима, поэтому для того, чтобы включить и настроить «мягкий режим», необходимо на уровне Сервера УД или группы клиентов во вкладке «Состояние» нажать кнопку «Неактивный режим».

Далее откроется окно «Настройка неактивного режима», где в правом нижем углу расположена кнопка «Мягкий режим». Она позволяет включать комбинацию настроек, при которых при обращении к ресурсам, доступ к которым запрещен, доступ все равно разрешается, но в журнал ресурсов заносится сообщение об ошибке.

События включения и выключения неактивного режима фиксируются в журнале управления политиками безопасности.

3.8 Наследование настроек

Дочерние объекты ВИ могут наследовать установленные настройки от родительской или принимать индивидуальные значения следующим образом:

1. Параметры, для которых отмечено наследование, примут значения, установленные для родительского объекта ВИ в дереве «Агенты ВИ». В этом случае параметры будут отображаться серым цветом.
2. Параметры, для которых выбраны и установлены оригинальные настройки, будут отображаться черным цветом.

Для того чтобы установить или снять наследование настроек имеются следующие возможности:

1. Чтобы параметры дочернего объекта наследовали значения, установленные для родительского объекта ВИ, необходимо на панели действий нажать кнопку «Наследовать настройки».
2. Если на панели действий нажать кнопку «Оригинальные настройки», то параметры дочернего объекта будут обозначены как индивидуально настроенные.

3.9 Значок блокировки на панели задач

После установки СЗИ ВИ на панели задач операционной системы у всех пользователей защищенного компьютера присутствует значок блокировки компьютера (рис. 105).

Двойной щелчок по значку мышкой позволит пользователю временно заблокировать компьютер. Разблокировка может быть произведена только пользователем, заблокировавшим компьютер.

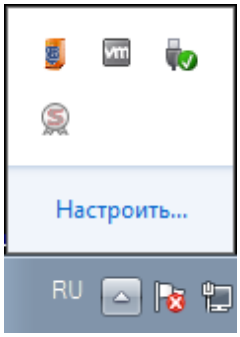


Рис. 105 – Контекстное меню значка блокировки

Щелчок правой кнопкой мыши по данному значку вызовет контекстное меню, через которое можно также задать ключ удаленного доступа (подробнее см. п. 5.6 «Ключи удаленного доступа»), посмотреть свойства пользователя и получить информацию о программе.

При выборе пункта «Свойства пользователя» появится окно с информацией об агенте управления доступом (рис. 106):

- Имя пользователя;
- Учетная запись;
- Описание (видно только администратору безопасности);
- Идентификатор сессии.

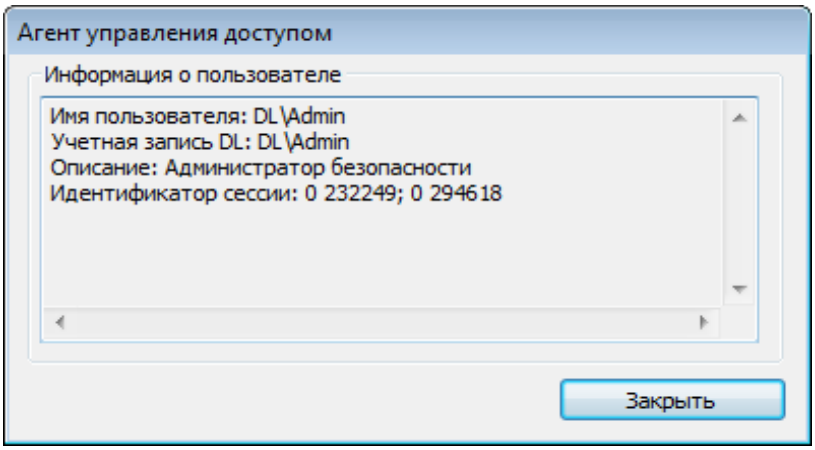


Рис. 106 – Свойства пользователя

4 ОПИСАНИЕ СРЕДСТВ АУДИТА

4.1 Веб-консоль

Просмотр установленных параметров безопасности, а также аудит журналов событий СЗИ ВИ можно осуществлять из веб-консоли СЗИ ВИ.

Веб-сервер устанавливается по умолчанию в процессе установки компонента ЦУ СЗИ ВИ Dallas Lock, представлен в виде службы.

Контроль доступа к веб-консоли ЦУ СЗИ ВИ осуществляется средствами ролевой модели разграничения доступа (подробнее см. п. 3.4 «Ролевая модель учетных записей СУД»).

Работа с веб-консолью осуществляется из окна браузера. Для вызова веб-консоли необходимо открыть браузер и в адресной строке ввести ip-адрес или полное доменное имя ТС с установленным компонентом ЦУ СЗИ ВИ Dallas Lock или, если доступ осуществляется непосредственно с ТС с установленным компонентом, указать в строке адреса localhost с указанием порта 6502. Например, 192.168.100.2:6502, szivi.dl.local:6502 или localhost:6502.

В окне авторизации требуется ввести следующие данные (рис. 107):

- Имя учетной записи (если учетная запись доменная, то необходимо указать домен);
- Пароль учетной записи пользователя.

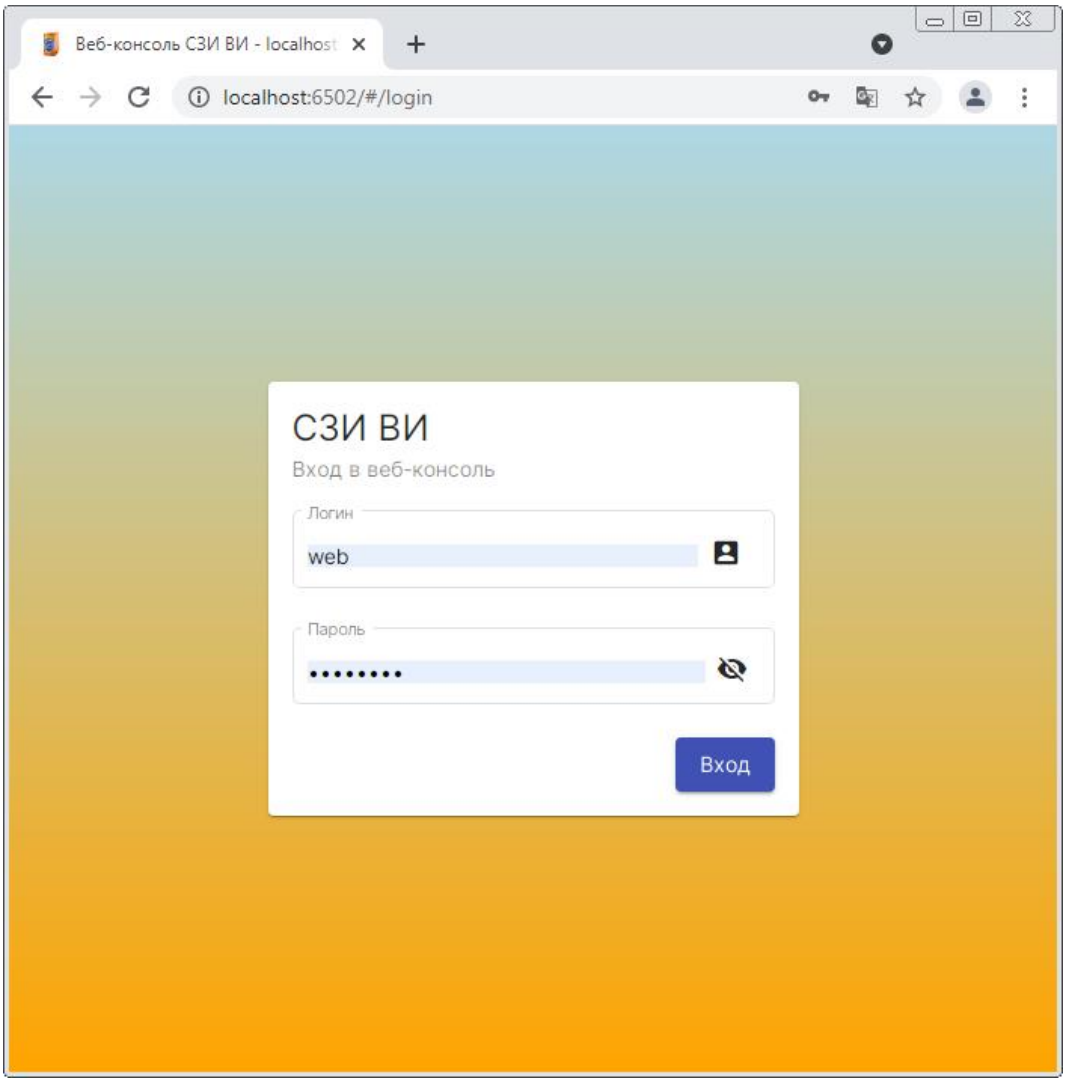


Рис. 107 – Вход в веб-консоль

Окно веб-консоли содержит следующие рабочие области (рис. 108):

1. Кнопка дополнительного меню.
2. Основное меню с набором вкладок.
3. Меню выбора пользователя.
4. Дополнительные вкладки основного меню
5. Меню действий.

6. Рабочая область, содержащая списки параметров или объектов текущей категории.
7. Вкладки выбора дерева (объектов DL и ВИ).
8. Проводник в виде дерева объектов, отображающий список клиентов, групп клиентов и объектов ВИ.

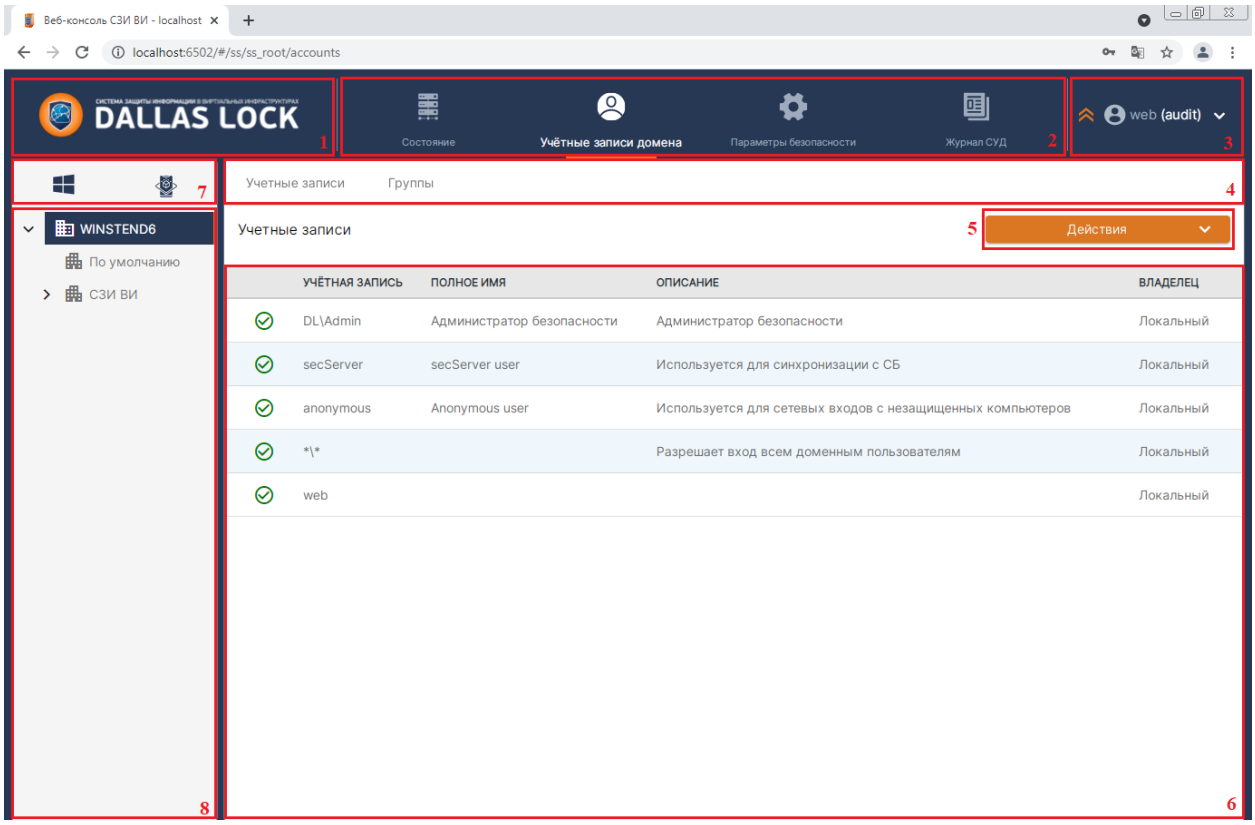


Рис. 108 – Основные элементы в веб-консоли

Для каждого из объектов в верхней части основного меню веб-консоли формируется свой список вкладок. При выборе вкладки в рабочей области открывается страница с соответствующими параметрами и меню.

4.2 Информационная панель

4.2.1 Дерево «Агенты Windows»

При выборе в дереве «Агенты Windows»  корневого элемента «Сервер УД» в рабочей области отображается следующая информация (Рис. 109):

1. наименование сервера УД (1);
2. количество событий НСД (зарегистрированных / не прочитанных) (2);
3. информация о версии продукта и пакете технической поддержки (3);
4. информация об агентах защиты (4);
5. блок выборки отображаемых данных по времени («день», «неделя», «месяц», «период») (5);
6. круговые диаграммы (события НСД по типу и по приоритету) (6).

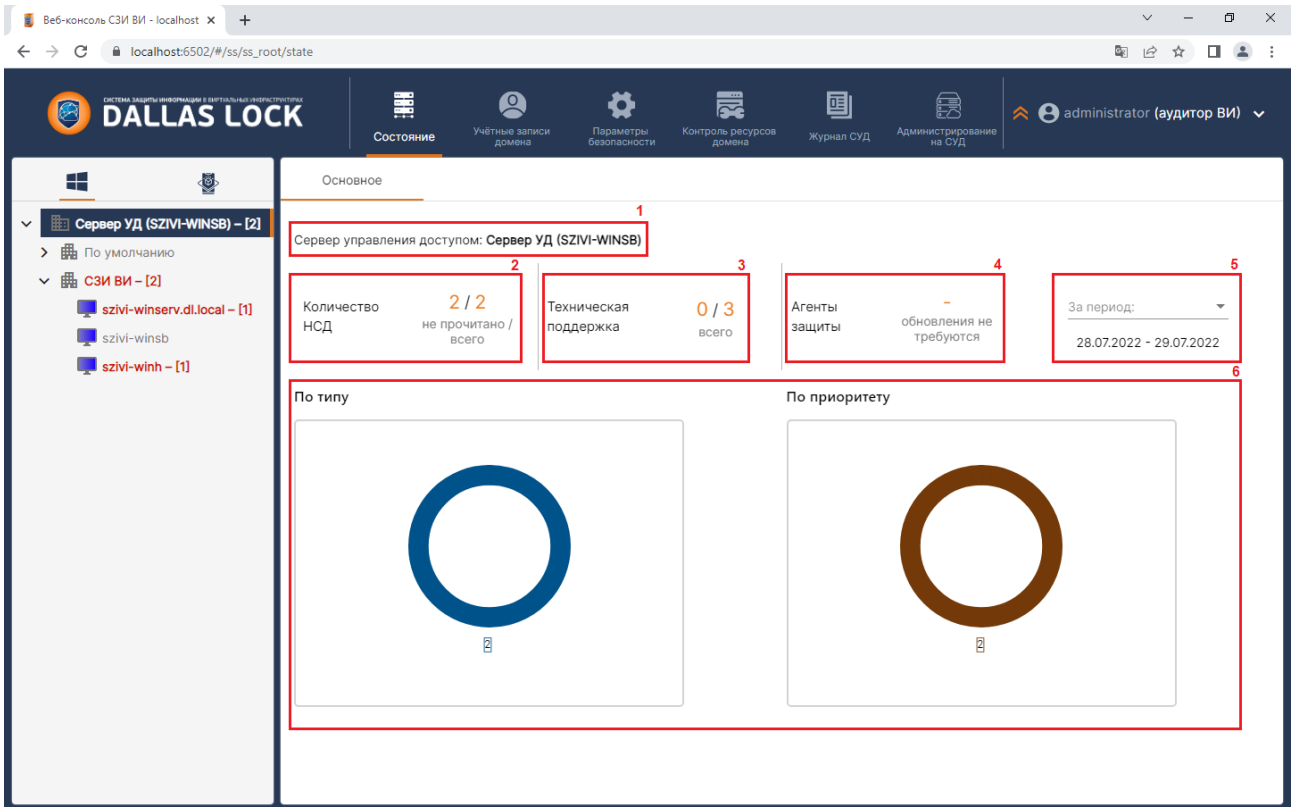


Рис. 109 – Сводная информация по элементу «Сервер УД» вкладки «Агенты Windows»

4.2.1.1 Информационная панель группы клиентов Windows

При выборе в дереве «Агенты Windows» группы клиентов в рабочей области отображается следующая информация (Рис. 110):

1. наименование группы (1);
2. количество событий НСД (зарегистрированных / не прочитанных) (2);
3. количество лицензий технической поддержки (3);
4. информация об агентах защиты на клиентах (4);
5. блок выборки отображаемых данных по времени («день», «неделя», «месяц», «период») (5);
6. круговые диаграммы (события НСД по типу и по приоритету) (6).

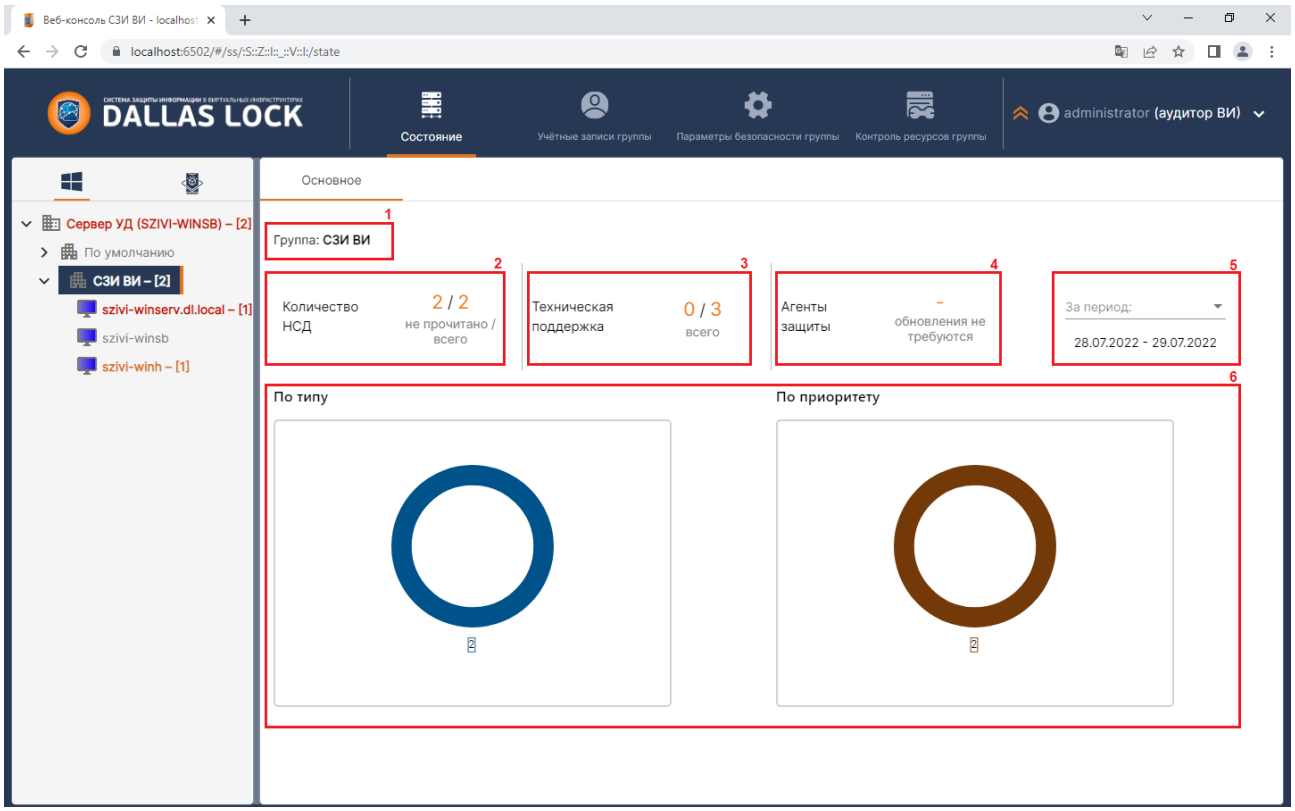


Рис. 110 – Сводная информация по группе клиентов Windows

4.2.1.2 Информационная панель клиентов Windows

При выборе в дереве «Агенты Windows» клиента Windows в рабочей области отображается следующая информация (Рис. 111):

1. имя клиента;
2. статус и версия агента DL;
3. компоненты;
4. статус неактивного режима;
5. наличие технической поддержки продукта;
6. количество сессий на клиенте;
7. количество событий НСД (зарегистрированных / не прочитанных);
8. блок выборки отображаемых данных по времени («день», «неделя», «месяц», «период»);

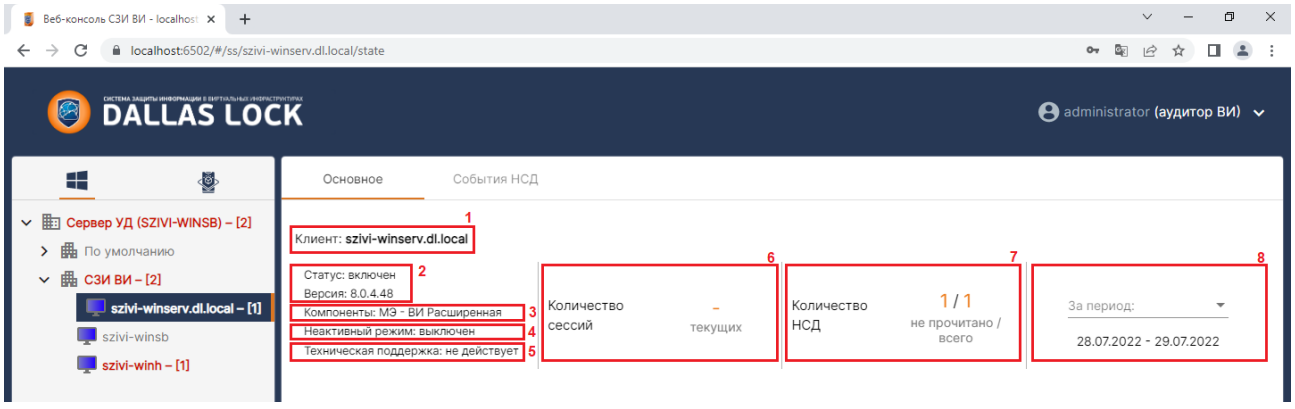


Рис. 111 – Сводная информация по клиенту Windows

4.2.2 Дерево «Агенты ВИ»

При выборе в дереве «Агенты ВИ»  корневого элемента «Сервер УД» в рабочей области отображается следующая информация (Рис. 112):

1. редакция и статус ЕЦУ;

2. информация о задействованных лицензиях (общее и по платформам);
3. блок выборки отображаемых данных по времени («день», «неделя», «месяц», «период»);
4. круговые диаграммы (события НСД по типу и по приоритету).

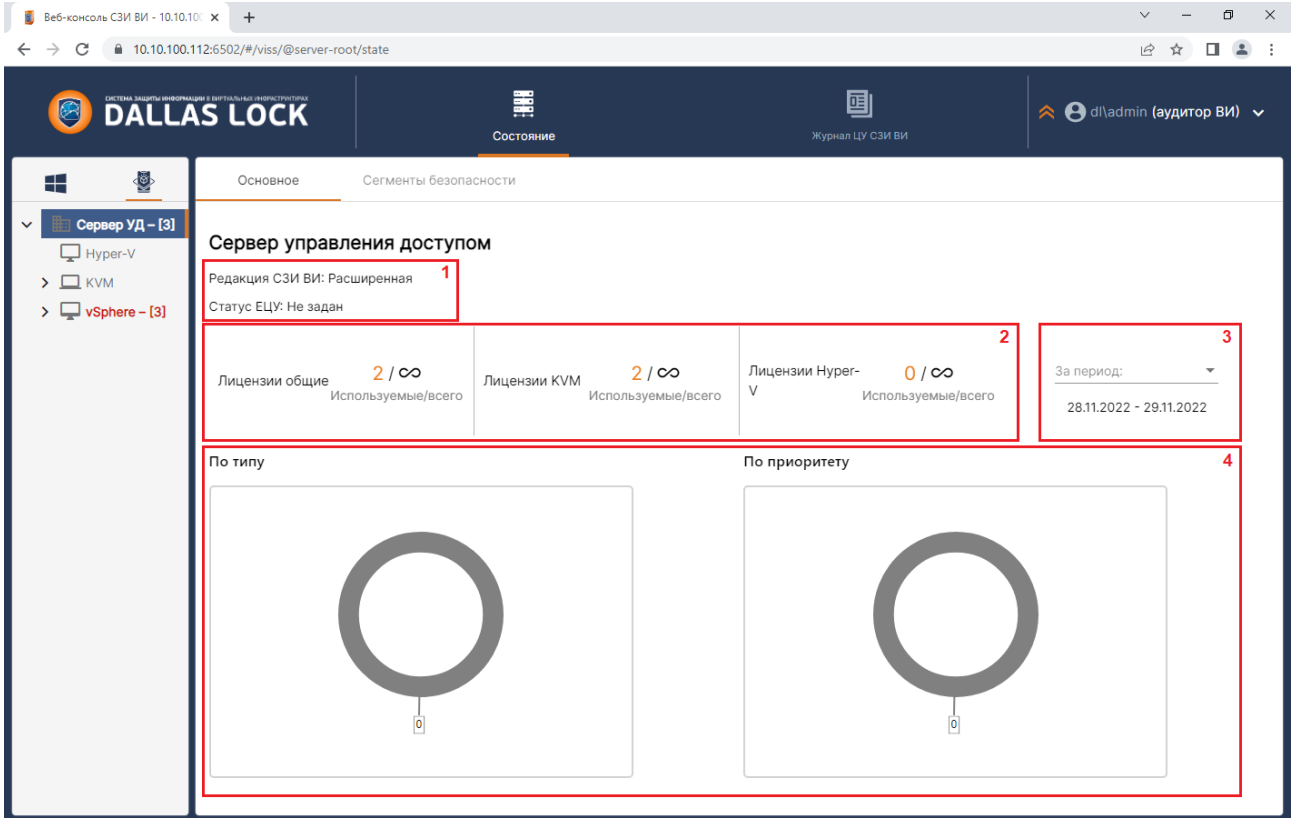


Рис. 112 – Сводная информация по элементу «Сервер УД» вкладки «Агенты ВИ»

4.2.2.1 Информационная панель групп ВИ

Группы элементов «vSphere», «Hyper-V» и «KVM» единообразно отображают информацию о себе. При выборе группы в дереве «Агенты ВИ» состояние объектов группы отображается в рабочей области (Рис. 113).

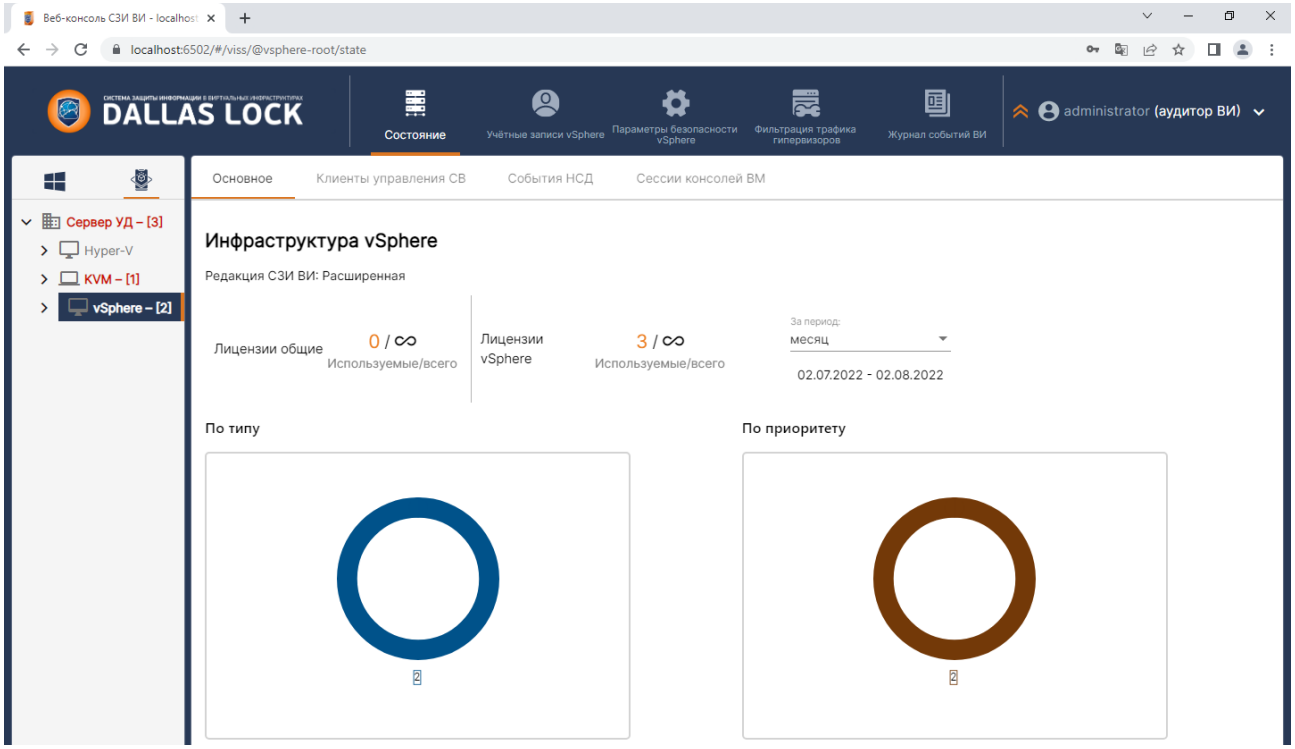


Рис. 113 – Сводная информация по группе vSphere

5 ПОДСИСТЕМА УПРАВЛЕНИЯ ПОЛЬЗОВАТЕЛЯМИ

5.1 Управление учетными записями

В СЗИ ВИ возможна регистрация пользователей следующих видов:

1. Пользователь, созданный средствами ОС Windows на СВ.
2. Пользователь, созданный средствами СЗИ ВИ на СВ.
3. Пользователей, созданных средствами службы Active Directory (если компьютер находится под управлением Контроллера домена).
4. Пользователь домена vSphere (например, vsphere.local, VSPHERE.COMMON).
5. Пользователь гипервизора.

Внимание! Если СЗИ ВИ Dallas Lock находится под управлением ЕЦУ и введен в ДБ ЕЦУ (подробнее см. п. 10 «ЕДИНЫЙ ЦЕНТР УПРАВЛЕНИЯ DALLAS LOCK») регистрация пользователей должна осуществляться в консоли ЕЦУ (С подробным описанием ЕЦУ Dallas Lock можно ознакомиться в Инструкции по использованию ЕЦУ Dallas Lock RU.48957919.501410-01 И6 / RU.48957919.501410-02 И6), в противном случае при синхронизации данные УЗ будут удалены, за исключением учетных записей, с параметром «не синхронизируемая» или «служебный пользователь» (подробнее см. п. 5.1.2 «Управление учетными записями клиентов Windows».

5.1.1 Полномочия на управление учетными записями

Регистрировать и удалять пользователей, а также просматривать и редактировать учетные записи может только пользователь, наделенный соответствующими полномочиями по администрированию.

Полномочиями для создания, удаления и изменения учетных записей пользователей в системе защиты обладают: суперадминистратор и пользователи (группы пользователей), указанные в списке разрешенных параметра «Параметры безопасности: Управление» (подробнее см. п. 5.4.1 «Полномочия на управление параметрами безопасности»).

5.1.2 Управление учетными записями клиентов Windows

Управление учетными записями клиентов Windows осуществляется в дереве «Агенты Windows».

5.1.2.1 Создание учетных записей Windows

Перед созданием новой учетной записи необходимо убедиться в том, что нужная учетная запись еще не создана в операционной системе. В таком случае, достаточно будет ее просто зарегистрировать, выбрав из списка, вызываемого кнопкой поиска.

Для создания нового пользователя в системе защиты необходимо:

1. Выбрать уровень Сервера УД и открыть вкладку «Учетные записи домена» → категория «Учетные записи» (рис. 114).

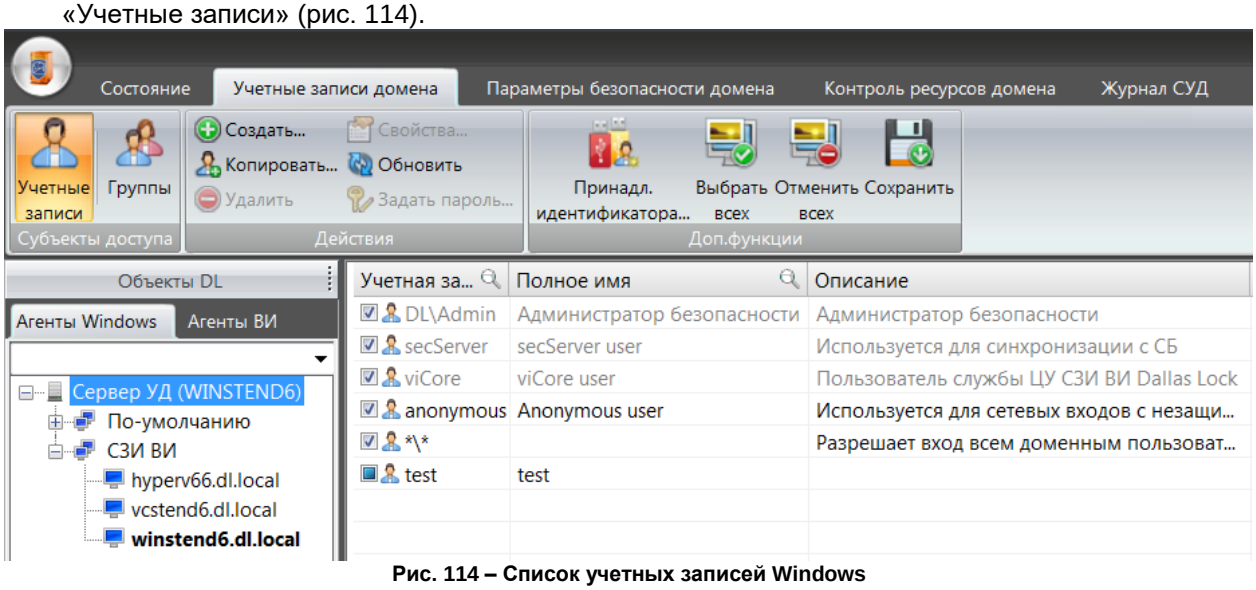


Рис. 114 – Список учетных записей Windows

2. Нажать кнопку «Создать».

3. В появившемся окне выбрать размещение «Локальный» и ввести имя учетной записи. При вводе имени в системе существуют следующие правила:

- максимальная длина имени – 20 символов;
- имя может содержать латинские символы, символы кириллицы, цифры и специальные символы (кроме запрещенных ОС: « / \ [ ] : | < > + = ; , ? @ *);
- разрешается использовать различные регистры клавиатуры, при этом регистр не учитывается, то есть заглавные и прописные буквы воспринимаются как одинаковые (User и user являются одинаковыми именами).

Кнопка поиска, расположенная рядом с полем логина, разворачивает список учетных записей пользователей, зарегистрированных в ОС данного ПК, и позволяет выбрать пользователя из уже существующих (рис. 115).

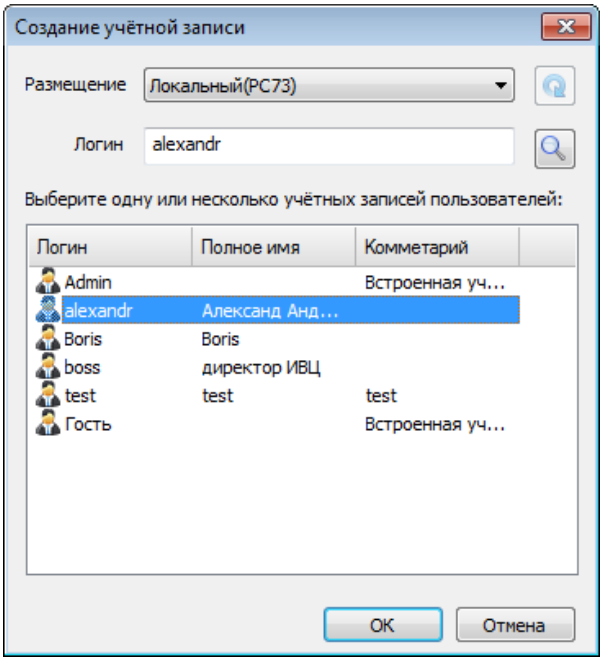


Рис. 115 – Учетные записи, зарегистрированные в ОС компьютера

Также можно выделить несколько учетных записей, имеющихся в ОС, и зарегистрировать их одновременно.

4. После нажатия «OK» появится окно редактирования параметров учетной записи (рис. 116).

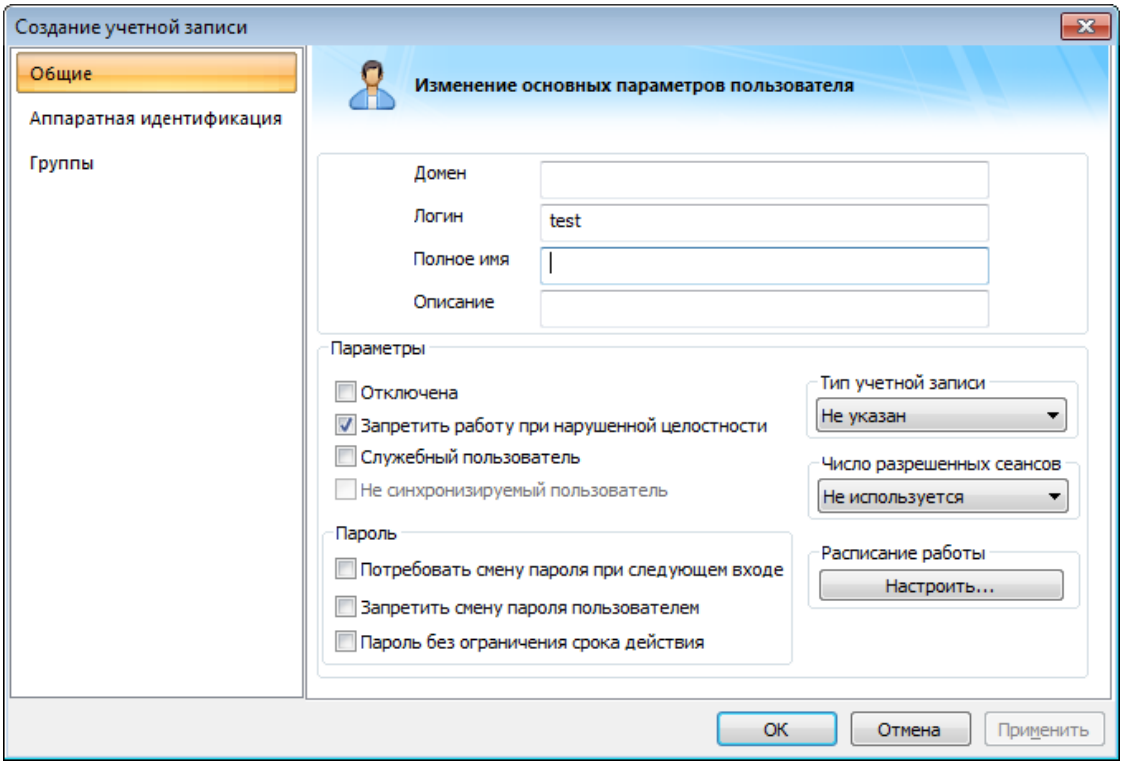


Рис. 116 – Окно редактирования параметров новой учетной записи

На вкладке «Общие» предлагается заполнить следующие учетные данные и параметры:

- Заполнить **«Полное имя»** пользователя.
- В поле «**Описание**» ввести любой комментарий. Длина комментария не более 256 символов. Вводить комментарий и полное имя не обязательно.
- Политики «**Отключена**» и «**Запретить работу при нарушении целостности**» задаются при необходимости:
  - Администратор имеет возможность отключить учетную запись любого пользователя, после чего пользователь не сможет войти на защищенный компьютер до тех пор, пока администратор не деактивирует эту опцию.
  - Система защиты обеспечивает проверку целостности программно-аппаратной среды ПК, объектов ФС и реестра. Если для пользователя опция «Запретить работу при нарушении целостности» активизирована, то при обнаружении нарушения целостности выдается соответствующее предупреждение и вход в ОС блокируется до тех пор, пока администратор не разблокирует учетную запись. Если же эта опция не включена, то при обнаружении нарушения целостности будет отображено только предупреждение.
- Флаг в поле «**Служебный пользователь**» предоставляет данной учетной записи особый статус. Требуется для корректной работы программ, при установке которых создаются свои учетные записи пользователей и осуществляется автоматический вход при загрузке ОС. Например, такой статус необходим при использовании программ VipNet или VMware. Пароль для данной УЗ можно задать
- Флаг в поле **«Не синхронизируемый пользователь»** при настройке учетных записей на уровне Сервера УД неактивно. Его настройка доступна при редакции параметров учетной записи пользователя на уровне клиента во вкладке «Учетные записи». Флаг в данном поле устанавливает статус, при котором данная учетная запись не синхронизируется с ЦУ СЗИ ВИ (см. п. 3.5 «Синхронизация»). Требуется для корректной работы программ, при установке которых создаются свои локальные учетные записи пользователей на клиентах Windows.
- Необходимо выбрать **«Тип учетной записи».** Для типа «Временный» обязательным условием является настройка расписания работы пользователя (см. ниже). По умолчанию тип учетной записи будет иметь значение «Не указан».
- Выбрать значение в поле **«Число разрешенных сеансов» в случае, если** это необходимо.

Примечание. При установленном значении числа разрешенных сеансов для каждой учетной записи (локальной или доменной) будет проверяться количество одновременных интерактивных и сетевых сессий (входов).

Если число больше установленного – вход пользователя на ПК запрещается. Если стоит ограничение для учетной записи по маске, ограничение будет действовать на каждого доменного пользователя индивидуально.

Таким образом, установив параметр «Число разрешенных сеансов» равным 1, можно настроить запрет вторичного (параллельного) входа пользователя в ОС.

- Необходимо задать «**Расписание работы»** пользователя, выбрать период и время. Вне указанного периода пользователь не сможет зайти на защищенный ПК. По окончании времени работы ПК пользователя будет заблокирован при условии включения на уровне Сервера УД параметра безопасности «Принудительное завершение работы по расписанию» («Параметры безопасности домена» → «Права пользователей»).
- Отмеченный параметр «**Потребовать смену пароля при следующем входе**» единовременно запросит смену пароля при входе.
- Поле «**Запретить смену пароля пользователем**».
- Флаг в поле «**Пароль без ограничения срока действия**» отменяет действие политики входа «Максимальный срок действия паролей», распространяемой на всех пользователей.

Примечание. Поле **«Логин»** и поле **«Домен»** остаются без возможности изменения (название домена для локального пользователя остается пустым).

Далее, в процессе создания или регистрации нового локального пользователя администратор имеет возможность включить его в определенную группу. В окне закладки «Группы» отображены названия групп, в которые включен пользователь (рис. 117). По умолчанию, каждый новый пользователь входит в группу «Пользователи».

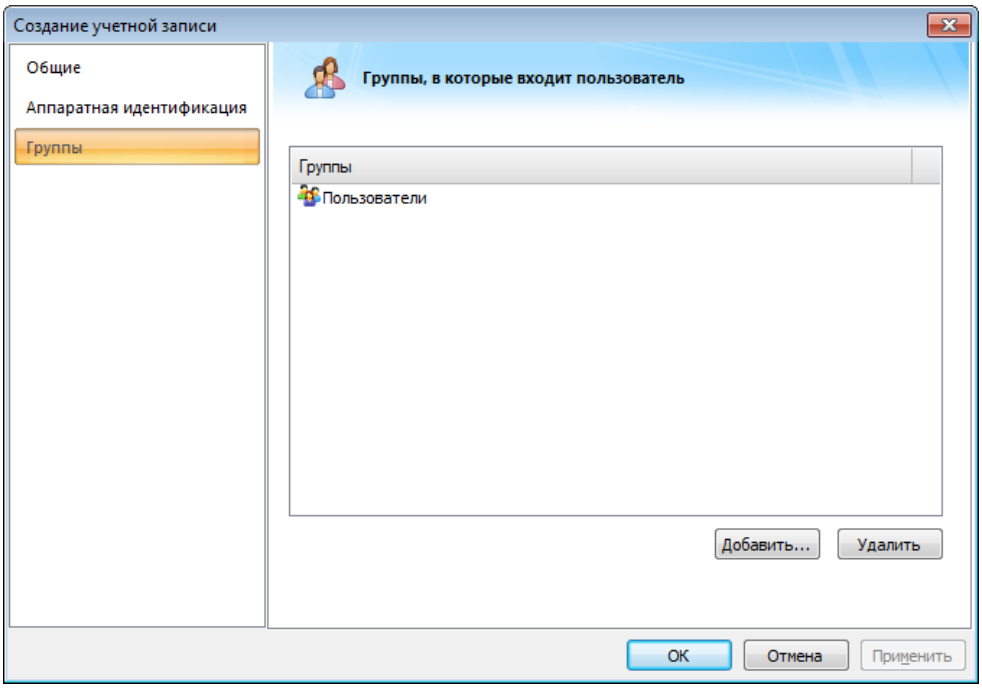


Рис. 117 – Окно редактирование списка групп пользователя

Примечание. Если для регистрации в СЗИ ВИ при выборе пользователей, имеющихся в ОС одновременно выделить несколько учетных записей, то для них настраиваются одинаковые свойства в одном окне.

5. Чтобы включить пользователя в определенную группу необходимо нажать «Добавить». Появится список всех групп пользователей, имеющихся в системе (кроме тех, в которые пользователь уже включен) (рис. 118).

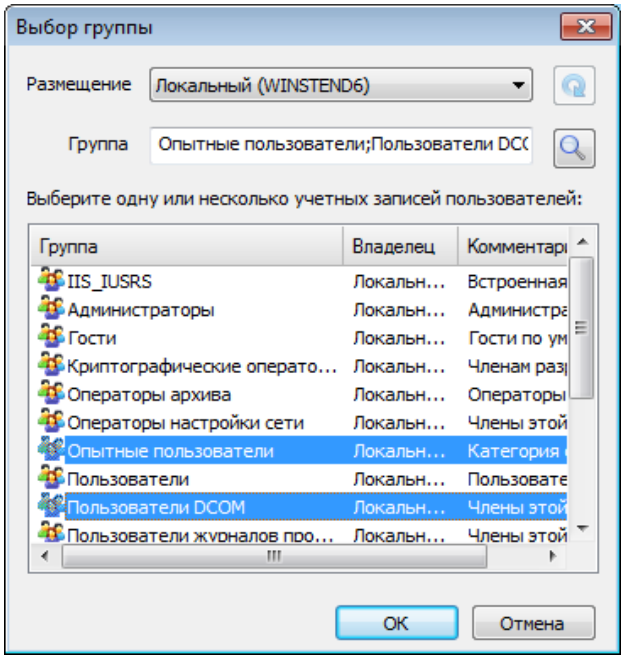


Рис. 118 – Окно выбора групп для учетной записи

6. В поле «Размещение» необходимо оставить значение «Локальный». В списке групп нужно выбрать необходимую. Одновременно можно выделить несколько групп в списке.

Кнопка поиска  в данном окне помогает найти необходимые группы по названию или его части. Возможна сортировка по алфавиту списка групп нажатием на поле с названием и со значком сортировки (треугольник).

7. Завершающей операцией по созданию учетной записи пользователя является назначение пароля. Назначение пароля предлагается системой защиты после заполнения всех необходимых параметров в окне создания учетной записи и нажатия кнопки «ОК» (рис. 119).

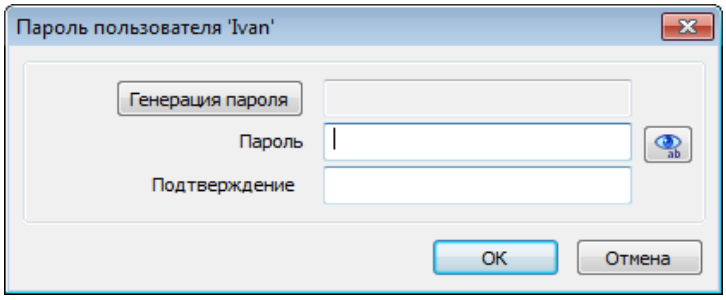


Рис. 119 – Форма ввода пароля

При вводе пароля необходимо руководствоваться следующими правилами:

- максимальная длина пароля 32 символа;
- пароль может содержать латинские символы, символы кириллицы, цифры и специальные символы (список допустимых символов см. в описании политики безопасности «Пароли: необходимо наличие спец. символов» в п.5.4.3 «Настройка параметров »);
- сложность пароля (наличие определенных символов, длина, срок действия и прочие) регулируется специальными политиками безопасности, которые устанавливаются администратором (см. п.5.4.3 «Настройка параметров »).

Для создания пароля, отвечающего всем установленным требованиям политик безопасности, можно воспользоваться помощью генератора паролей системы защиты. Для этого нажать кнопку с надписью «Генерация пароля». Система автоматически создаст случайный пароль, удовлетворяющий политикам сложности пароля, значение которого необходимо ввести в поля «Пароль» и «Подтверждение».

Дополнительная кнопка  изменит скрытые символы на явные. Подтверждение пароля в этом случае не потребуется и соответствующее поле будет скрыто.

Примечание. Если в СЗИ ВИ регистрируется пользователь, учетная запись которого уже имеется на локальном компьютере, то его пароль для входа в ОС автоматически становится паролем для входа в систему защиты, поэтому операция по назначению пароля не предлагается. При необходимости пароль можно изменить средствами СЗИ ВИ.

Примечание. После того, как пользователь зарегистрирован, менять его имя средствами ОС не рекомендуется. В противном случае, доступ на компьютер с установленной системой защиты данному пользователю будет ограничен.

Также следует учесть, если учетная запись (в том числе в составе группы) отмечена в значении для параметра «Учетные записи: Принудительная двухфакторная аутентификация» (подробнее см. п. 5.5.2 «Принудительная двухфакторная аутентификация»), то присвоение аппаратного идентификатора станет обязательным условием, иначе при завершении ее регистрации или редактировании в СЗИ ВИ появится предупреждение об ошибке. Это правило распространяется для вновь создаваемых учетных записей пользователей.
Для использования созданной учетной записи требуется ее активация (подробнее см. п. 5.1.4 «Активация и деактивация учетных записей»).
Изменения вступят в силу при следующей синхронизации (подробнее п. 3.5 «Синхронизация»).

Создание учетных записей Windows путем копирования

При создании учетной записи пользователя, которая имеет одинаковые свойства с другой учетной записью, можно воспользоваться функцией копирования. Для этого необходимо выбрать учетную запись в списке и нажать «Копировать» на панели действий (рис. 120). Данные действия доступны на уровне сервера УД, на уровне группы клиентов и на уровне клиента.

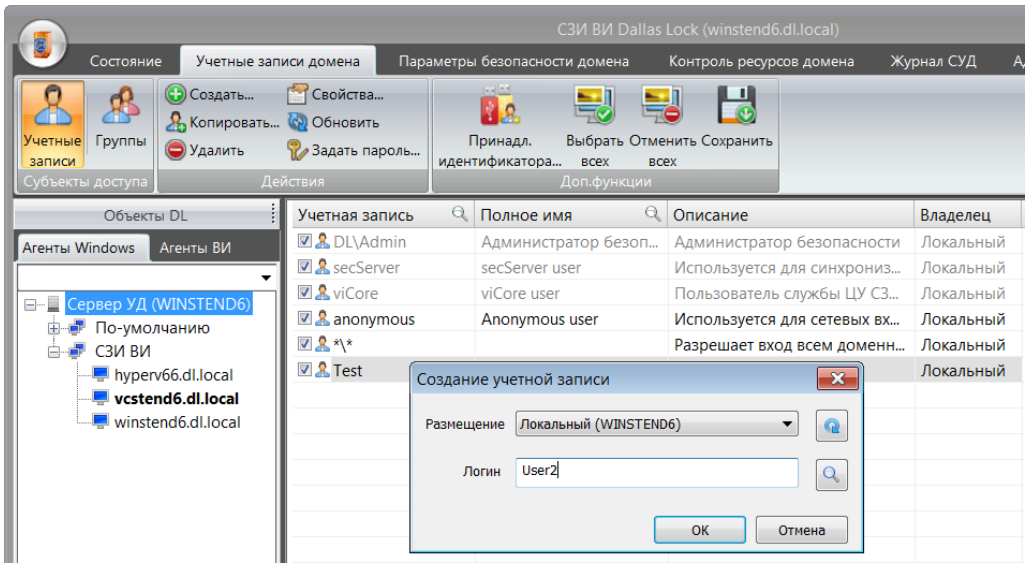


Рис. 120 – Создание новой учетной записи с копирование свойств

В появившемся окне ввести имя учетной записи. Далее, в окне свойств для создаваемой учетной записи будут установлены свойства и список групп с копируемой учетной записи, их можно отредактировать. Далее необходимо задать пароль.

Установка параметров доступа на ресурсы не копируется и осуществляется индивидуально для данной учетной записи (или для группы, в которую она входит).

Для использования созданной учетной записи требуется ее активация (подробнее см. п. 5.1.4 «Активация и деактивация учетных записей»).

Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

Редактирование учетных записей Windows

Для редактирования необходимо выбрать учетную запись из списка и двойным кликом вызвать окно редактирования параметров учетной записи, либо нажать кнопку «Свойства» или выбрать соответствующий пункт из контекстного меню. Дальнейшие действия полностью идентичны действиям, описанным в п. 5.1.2.1 «Создание учетных записей Windows» начиная с п. 5. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

5.1.2.2 Регистрация доменных учетных записей

Для того чтобы зарегистрировать в СЗИ ВИ учетную запись доменного пользователя, необходимо выполнить следующее.

1. Открыть дерево «Агенты Windows».
2. Выбрать уровень «Сервера УД» и открыть категорию «Учетные записи домена» → «Учетные записи».
3. Нажать кнопку «Создать».
4. В выпадающем меню размещения выбрать имя домена и нажать кнопку поиска (рис. 121).

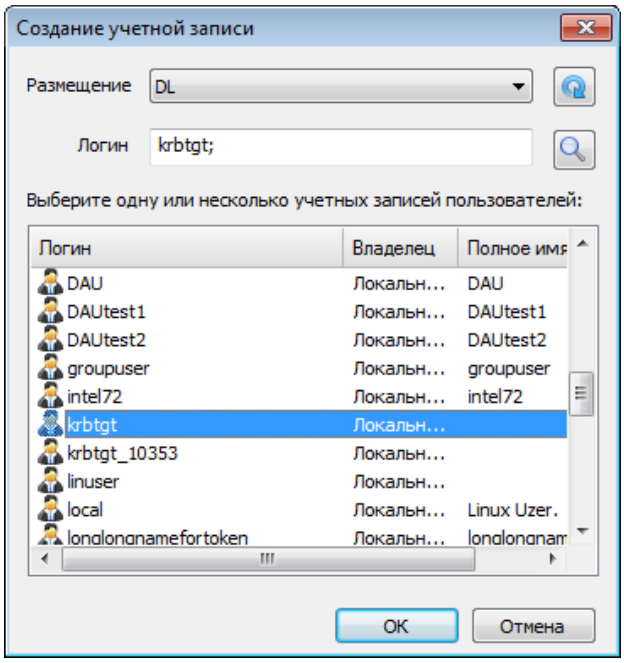


Рис. 121 – Заполнение имени учетной записи

Для получения списка учетных записей домена необходимо дополнительно ввести авторизационные данные администратора домена. После авторизации появится список пользователей, зарегистрированных на контроллере домена. Для поиска необходимой записи можно воспользоваться сортировкой или ввести первые буквы и нажать кнопку поиска  .

5. Выбрать учетную запись пользователя и нажать «ОК». Можно выделить несколько учетных записей, имеющихся в ОС, и зарегистрировать их одновременно.

В системе защиты автоматически сформируется учетная запись пользователя с теми параметрами, которые соответствуют ей на контроллере домена (имя домена, логин, пароль, полное имя, название групп на контроллере домена). Автоматически учетная запись пользователя в списке учетных записей будет иметь вид: «имя домена/имя пользователя».

Имеющихся доменных пользователей можно зарегистрировать в СЗИ ВИ, но их нельзя создать средствами СЗИ ВИ. Если нужен новый доменный пользователь, его придется создать средствами администрирования на контроллере домена, и только после этого зарегистрировать в СЗИ ВИ.

Список доменных пользователей и групп кэшируется СЗИ ВИ в своей памяти. Поэтому, если новый пользователь создан на контроллере домена, он может появиться в списке системы защиты не сразу. Необходимо обновить список с помощью кнопки «Обновить».

Примечание. Процесс получения списка доменных пользователей может быть достаточно длительным. Во время этого процесса возможно появление окошка с просьбой ввести идентификационную информацию администратора.

Примечание. Аппаратный идентификатор может быть назначен только для отдельно взятой доменной учетной записи, зарегистрированной в системе защиты, без маски.

Также средствами СЗИ ВИ невозможно изменить список групп, в которые входит доменный пользователь.

Для использования созданной учетной записи требуется ее активация (подробнее см. п. 5.1.4 «Активация и деактивация учетных записей»).

Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

5.1.2.3 Регистрация доменных учетных записей по маске

В СЗИ ВИ реализован механизм регистрации доменных учетных записей пользователей системы с использованием масок, по символу «*». В этом контексте символ «*» имеет значение «все».

Учетная запись «Имя_домена*» означает всех пользователей данного домена.

По такой маске возможна регистрация только доменных учетных записей, для локальных это невозможно, и каждая запись должна быть создана отдельно. В то же время, если известен пароль локального пользователя, ЦУ СЗИ ВИ (см. ниже) сможет такого пользователя создать на клиенте.

При установке СЗИ ВИ с конфигурацией по умолчанию, если ПК является членом домена Windows, в системе защиты автоматически регистрируется учетная запись «**». Это означает, что вход на защищенный компьютер могут осуществлять все доменные пользователи (в том числе пользователи доверенных доменов).

Механизм регистрации доменных учетных записей системы с использованием масок позволяет привести систему входа к строгому виду.

Каждая учетная запись может быть в состоянии «вход разрешен» и «вход запрещен». Чтобы запретить вход под соответствующей учетной записью, необходимо, чтобы был поставлен флаг в поле «Отключена» в окне параметров учетных записей (рис. 122).

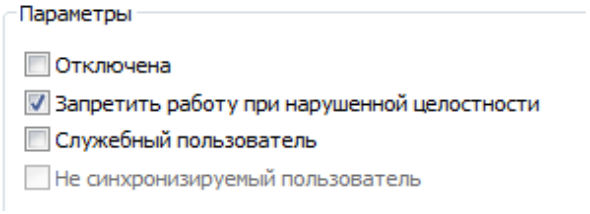


Рис. 122 – Окно редактирования учетной записи

Если для существующей учетной записи вида «**» запретить вход в систему, и одновременно разрешить вход для учетных записей типа «ZCB*», то в систему защиты пользователи доменов входить не смогут, но смогут входить только пользователи домена ZCB. Другой пример: если запретить вход в систему для записи «ZCB*», и разрешить для «ZCB\admin1», «ZCB\admin2», то это будет означать, что из домена ZCB на защищенный системой компьютер смогут входить только пользователи admin1 и admin2.

Таким образом, систему проверки пользователей можно легко привести к «строгой» системе, достаточно отключить учетную запись «**», и, далее, в явном виде регистрировать учетные записи необходимых доменных пользователей.

Примечание. Если в СЗИ ВИ зарегистрирована доменная учетная запись «**» или «Имя_домена*», то назначать права на доступ к объекту можно как для учетной записи «**» (или «Имя_домена*»), так и для каждой индивидуальной учетной записи домена, выбрав ее из списка через дескриптор объекта (см. ниже).

5.1.2.4 Сессии-исключения

Для корректной работы в режиме совместимости со сторонним ПО в СЗИ ВИ Dallas Lock реализован механизм регистрации сессий, которым в качестве исключения разрешается работа с ФС, несмотря на отсутствие явного санкционированного входа.

Зарегистрированные в СЗИ ВИ сессии называются сессии-исключения. СЗИ ВИ уже содержит список настроенных сессий первой необходимости. По умолчанию они отключены, кроме необходимых для работы Hyper-V и vCenter.

Для просмотра списка сессий-исключений и добавления новых, необходимо в дереве «Агенты Windows» на уровне клиента открыть вкладку «Состояние» в блоке «Действия с клиентом» либо из контекстного меню, вызываемого щелчком правой кнопки мыши, нажать кнопку «Подключиться».

После этого во вкладке «Учетные записи» или «Состояние» станет активна кнопка «Сессии-исключения» (рис. 123).

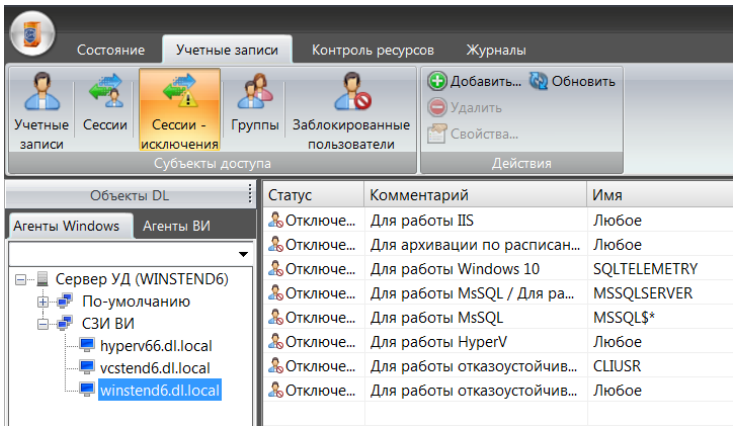


Рис. 123 – Сессии-исключения

Чтобы зарегистрировать в СЗИ ВИ сессию, необходимо нажать кнопку «Добавить». В появившемся окне ввести параметры сессии.

Добавленную в список сессию можно временно отключить, не удаляя из списка, и заново включить. Для этого в окне параметров сессии необходимо отметить флагом поле «Исключение активно» (рис. 124).

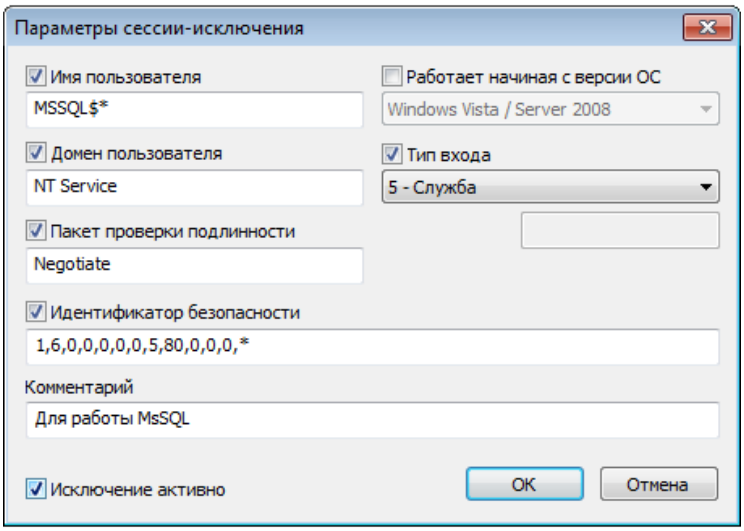


Рис. 124 – Редактирование параметров сессии-исключения

Удалять из списка зарегистрированные по умолчанию в СЗИ ВИ сессии-исключения не рекомендуется.

5.1.3 Управление учетными записями ВИ

Управление учетными записями ВИ осуществляется в дереве «Агенты ВИ».

5.1.3.1 Создание учетных записей vSphere

Для того чтобы создать учетную запись серверов виртуализации необходимо:

1. Выбрать уровень vSphere и открыть категорию «Учетные записи vSphere» → «Учетные записи vSphere» (рис. 125).

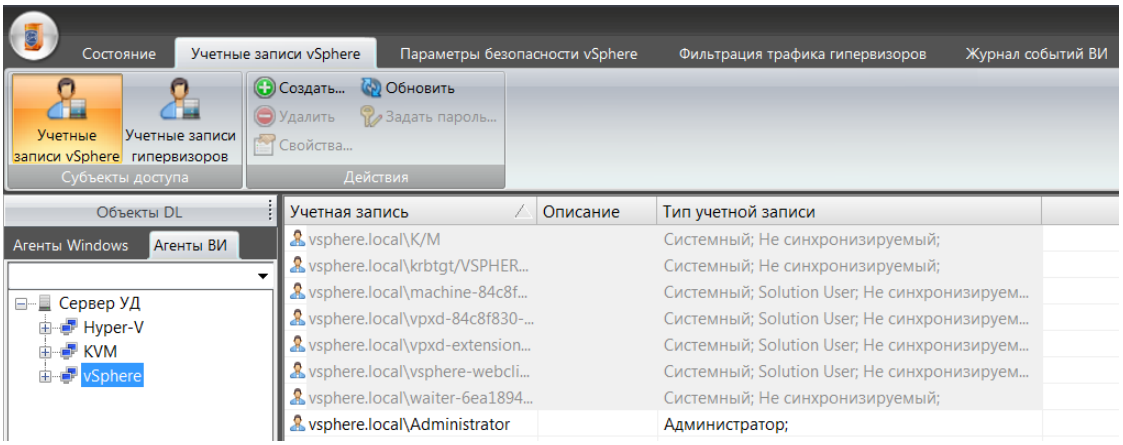


Рис. 125 – Список учетных записей vSphere

2. В категории «Действия» нажать кнопку «Создать».
3. В появившемся окне необходимо выбрать объект дерева ВИ, парольные политики которого необходимо использовать при проверке пароля создаваемой учетной записи, после чего нажать «ОК» (рис. 126).

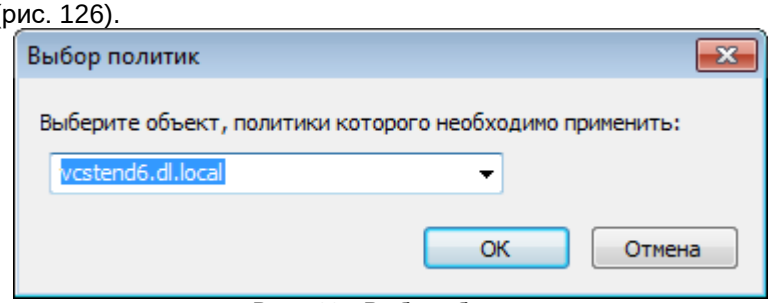


Рис. 126 – Выбор объекта

4. В появившемся окне ввести имя учетной записи, выбрать домен и заполнить остальные поля при необходимости, после чего нажать кнопку «ОК» (рис. 127).

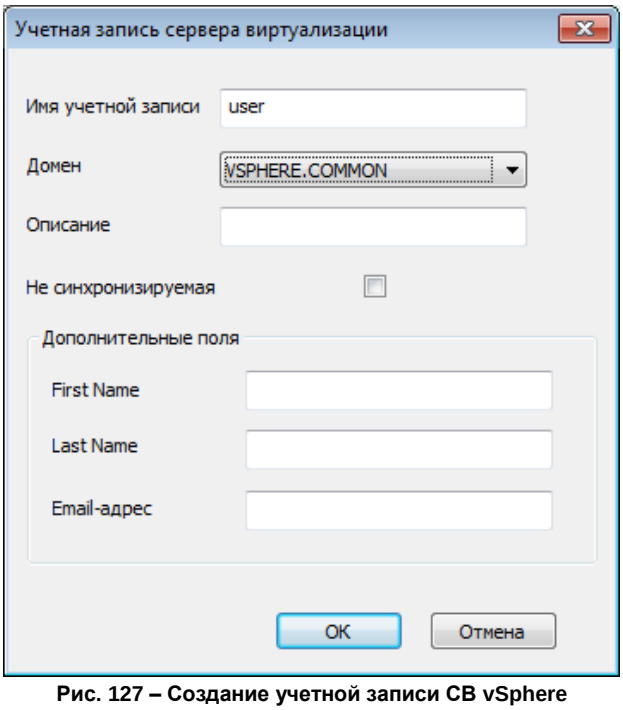


Рис. 127 – Создание учетной записи СВ vSphere

При вводе имени в системе существуют следующие правила:

- максимальная длина имени – 20 символов;
- имя может содержать латинские символы, символы кириллицы, цифры и специальные символы (кроме запрещенных: « / \ [ ] : | < > + = ; , ? @ * #);
- разрешается использовать различные регистры клавиатуры, при этом регистр не учитывается, то есть заглавные и прописные буквы воспринимаются как одинаковые (User и user являются одинаковыми именами).

5. Далее следует назначить пароль, который соответствует заданным парольным политикам (рис. 128).

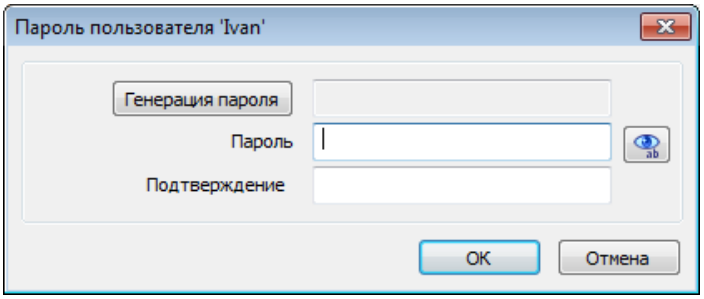


Рис. 128 – Форма ввода пароля

При вводе пароля необходимо руководствоваться следующими правилами:

- максимальная длина пароля 32 символа;
- пароль может содержать латинские символы, символы кириллицы, цифры и специальные символы (список допустимых символов см. в описании политики безопасности «[Сервер виртуализации] Пароли: минимальное количество специальных символов» в п. 5.3.1.1 «Параметры входа для vSphere»);
- сложность пароля (наличие определенных символов, длина, срок действия и прочие) регулируется специальными политиками безопасности, которые устанавливаются администратором (см. п. 5.3.1.1 «Параметры входа для vSphere»).

Для создания пароля, отвечающего всем установленным требованиям политик безопасности, можно воспользоваться помощью генератора паролей системы защиты. Для этого нажать кнопку «Генерация пароля». Система автоматически создаст случайный пароль, удовлетворяющий парольным политикам сложности пароля выбранного объекта дерева ВИ, значение которого необходимо ввести в поля «Пароль» и «Подтверждение».

Дополнительная кнопка  изменит скрытые символы на явные. Подтверждение пароля в этом случае не потребуется и соответствующее поле будет скрыто.

Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

Далее следует активировать учетную запись на уровне соответствующих СВ (подробнее см. п. 5.1.4 «Активация и деактивация учетных записей»).

5.1.3.2 Создание учетных записей гипервизора ESXi

Для того чтобы создать учетную запись гипервизора необходимо:

1. Выбрать уровень «vSphere» и открыть категорию «Учетные записи vSphere» → «Учетные записи гипервизоров» (рис. 129).

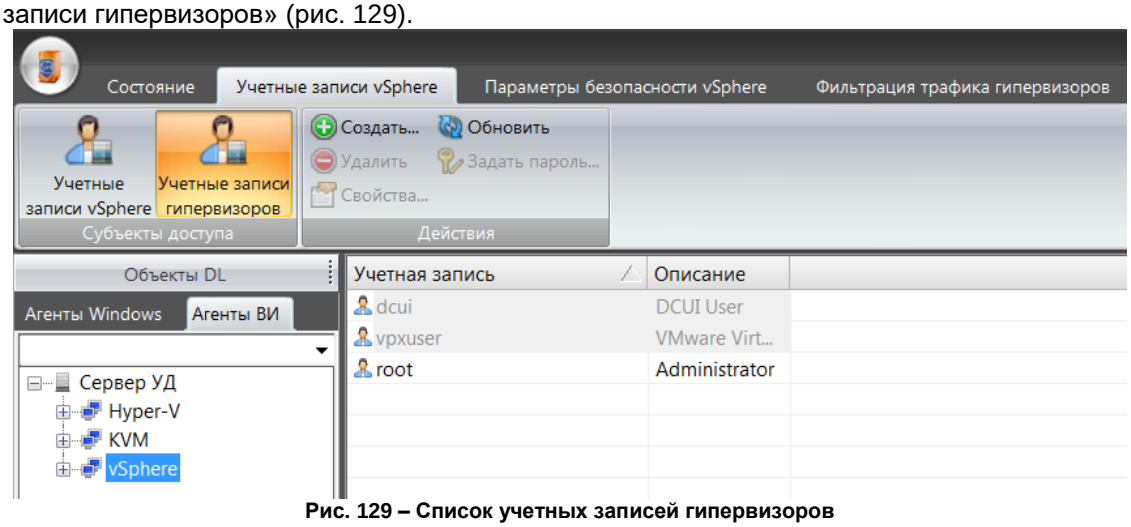


Рис. 129 – Список учетных записей гипервизоров

2. Нажать кнопку «Создать».
3. В появившемся окне выбрать объект, для которого будет создана учетная запись и нажать кнопку «ОК».
4. Далее в окне ввести имя учетной записи и заполнить поле «Описание» при необходимости, после чего нажать кнопку «ОК» (рис. 130).

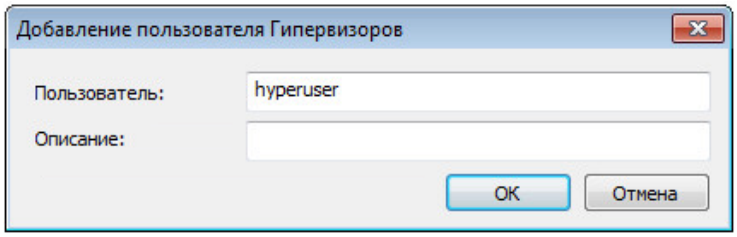


Рис. 130 – Создание пользователя гипервизора ESXi

При вводе имени в системе существуют следующие правила:

- максимальная длина имени – 20 символов;
- имя может содержать латинские символы, символы кириллицы, цифры и специальные символы (кроме запрещенных: « / \ [ ] : | < > + = ; , ? @ * #);
- разрешается использовать различные регистры клавиатуры, при этом регистр не учитывается, то есть заглавные и прописные буквы воспринимаются как одинаковые (User и user являются одинаковыми именами).

5. Далее следует назначить пароль, который соответствует заданным парольным политикам (рис. 131).

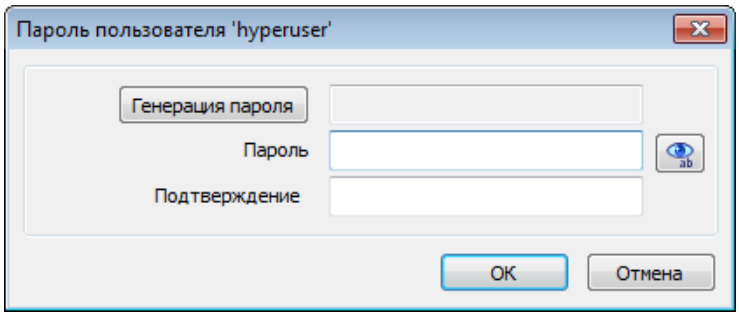


Рис. 131 – Форма ввода пароля

При вводе пароля необходимо руководствоваться следующими правилами:

- максимальная длина пароля 32 символа;
- пароль может содержать латинские символы, символы кириллицы, цифры и специальные символы (список допустимых символов см. в описании политики безопасности «[Сервер виртуализации] Пароли: минимальное количество специальных символов» в п. 5.3.1.1 «Параметры входа для vSphere»);
- сложность пароля (наличие определенных символов, длина, срок действия и прочие) регулируется специальными политиками безопасности, которые устанавливаются администратором (см. п. 5.3.1.1 «Параметры входа для vSphere»).

Для создания пароля, отвечающего всем установленным требованиям политик безопасности, можно воспользоваться помощью генератора паролей системы защиты. Для этого нажать кнопку «Генерация пароля». Система автоматически создаст случайный пароль, удовлетворяющий политикам сложности пароля, значение которого необходимо ввести в поля «Пароль» и «Подтверждение».

Дополнительная кнопка  изменит скрытые символы на явные. Подтверждение пароля в этом случае не потребуется и соответствующее поле будет скрыто.

6. Для использования созданной учетной записи требуется ее активация (подробнее см. п. 5.1.4 «Активация и деактивация учетных записей»).

7. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

5.1.3.3 Создание учетных записей гипервизора KVM

Для того чтобы создать учетную запись гипервизора необходимо:

1. Выбрать уровень гипервизора «KVM» и открыть вкладку «Системные учетные записи» → «Доступ к авторизации» (рис. 132).

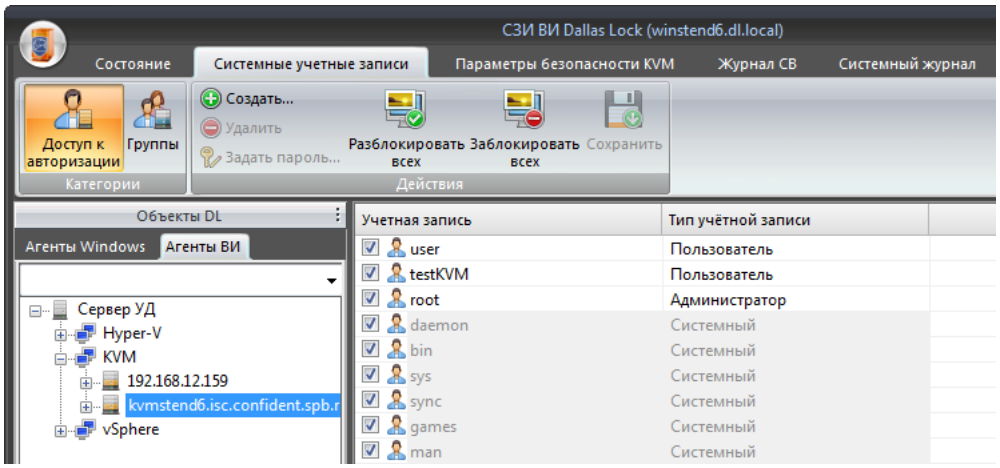


Рис. 132 – Список учетных записей KVM

2. Нажать кнопку «Создать».
3. В появившемся окне ввести имя учетной записи, после чего нажать кнопку «ОК» (рис. 133).

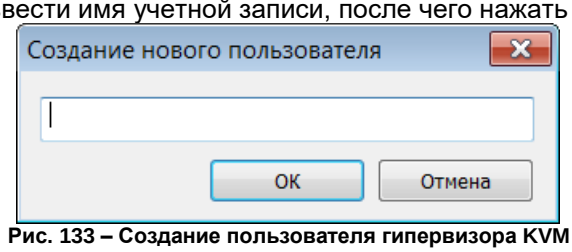


Рис. 133 – Создание пользователя гипервизора KVM

4. Далее следует назначить пароль (рис. 134).

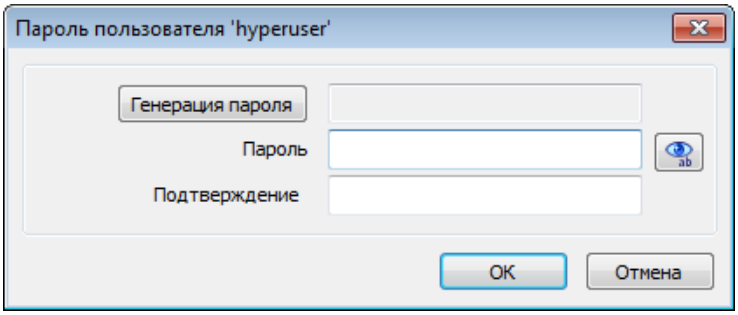


Рис. 134 – Форма ввода пароля

Для создания пароля, отвечающего всем установленным требованиям политик безопасности, можно воспользоваться помощью генератора паролей системы защиты. Для этого нажать кнопку «Генерация пароля». Система автоматически создаст случайный пароль, удовлетворяющий политикам сложности пароля, значение которого необходимо ввести в поля «Пароль» и «Подтверждение».

Дополнительная кнопка  изменит скрытые символы на явные. Подтверждение пароля в этом случае не потребуется и соответствующее поле будет скрыто.

5. Далее необходимо нажать кнопку «Сохранить».
6. Для использования созданной учетной записи требуется ее активация (подробнее см. п. 5.1.4 «Активация и деактивация учетных записей»).
7. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

Примечание. Для предоставления доступа новому пользователю к управлению ВМ необходимо добавить данного пользователя в следующие группы:

1. Для ОС Linux Mint – libvirt.
2. Для ОС Ubuntu – libvirt, kvm.
3. Для ОС Astra Linux (Орел 2.12) – kvm, libvirt, libvirt-qemu.
4. Для ОС Astra Linux (Смоленск 1.6) – kvm, libvirt, libvirt-qemu, libvirt-admin.
5. Для ОС CentOS – kvm.

5.1.3.4 Создание учетных записей oVirt/zVirt/HOSTVM/РЕД Вирт

Для того чтобы создать учетную запись сервера виртуализации необходимо:

1. Выбрать уровень СВ oVirt/zVirt/HOSTVM/РЕД Вирт и открыть категорию «Учетные записи oVirt/zVirt/HOSTVM/РЕД Вирт» → «Учетные записи» (рис. 135).

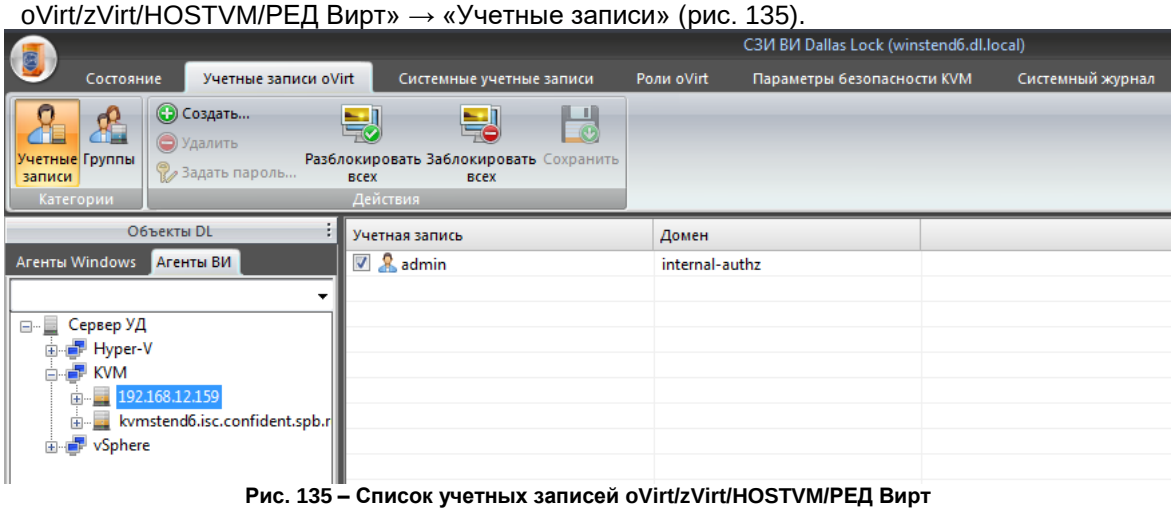


Рис. 135 – Список учетных записей oVirt/zVirt/HOSTVM/РЕД Вирт

2. В категории «Действия» нажать кнопку «Создать».
3. В появившемся окне ввести имя учетной записи, после чего нажать кнопку «ОК» (рис. 136).

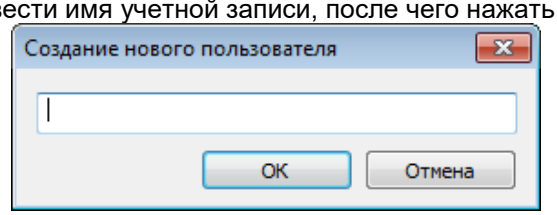


Рис. 136 – Создание учетных записей oVirt/zVirt/HOSTVM/РЕД Вирт

4. Далее следует назначить пароль

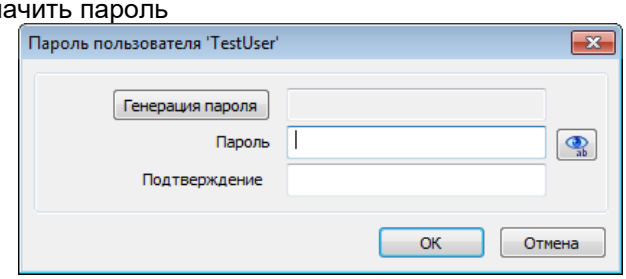


Рис. 137 – Создание учетных записей oVirt/zVirt/HOSTVM/РЕД Вирт

Для создания пароля, отвечающего всем установленным требованиям политик безопасности, можно воспользоваться помощью генератора паролей системы защиты. Для этого нажать кнопку «Генерация пароля». Система автоматически создаст случайный пароль, удовлетворяющий политикам сложности пароля, значение которого необходимо ввести в поля «Пароль» и «Подтверждение».

Дополнительная кнопка  изменит скрытые символы на явные. Подтверждение пароля в этом случае не потребуется и соответствующее поле будет скрыто.

5. Далее необходимо нажать кнопку «Сохранить».
6. Для использования созданной учетной записи требуется ее активация (подробнее см. п. 5.1.4 «Активация и деактивация учетных записей»).
7. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

5.1.3.5 Создание локальных учетных записей oVirt/zVirt/HOSTVM/РЕД Вирт

Для того чтобы создать локальную учетную запись СВ или гипервизора необходимо:

1. Выбрать уровень СВ или гипервизора oVirt/zVirt/HOSTVM/РЕД Вирт и открыть вкладку «Системные учетные записи» → «Доступ к авторизации» (рис. 138).

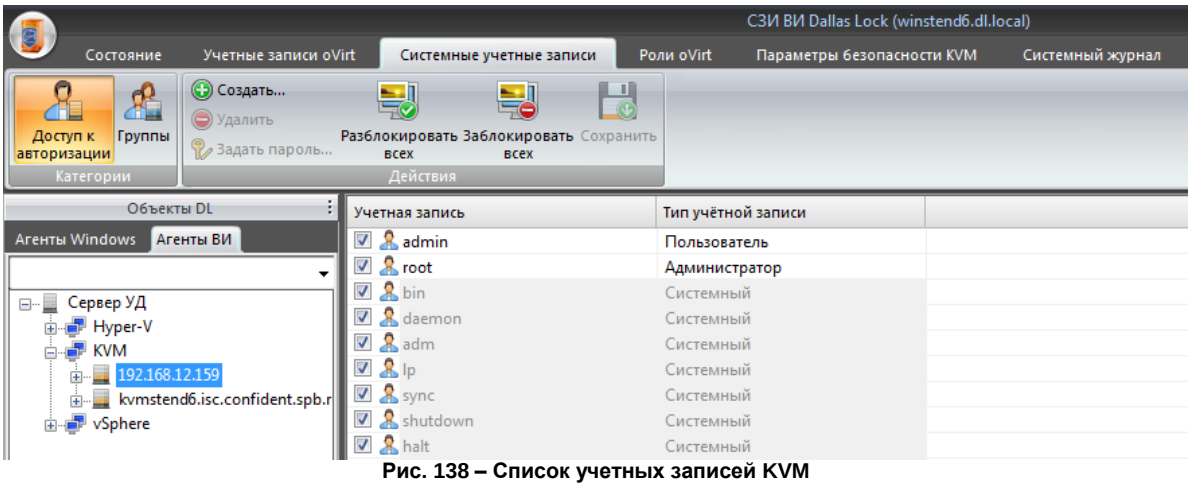


Рис. 138 – Список учетных записей KVM

2. Нажать кнопку «Создать».
3. В появившемся окне ввести имя учетной записи, после чего нажать кнопку «ОК» (рис. 139).

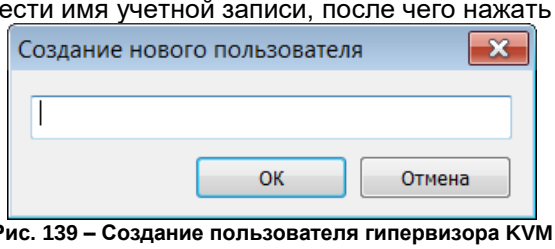


Рис. 139 – Создание пользователя гипервизора KVM

4. Далее следует назначить пароль (рис. 140).

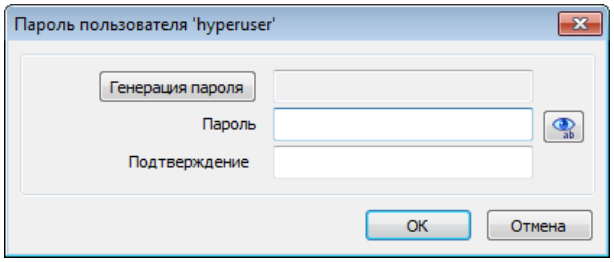


Рис. 140 – Форма ввода пароля

Для создания пароля, отвечающего всем установленным требованиям политик безопасности, можно воспользоваться помощью генератора паролей системы защиты. Для этого нажать кнопку «Генерация пароля». Система автоматически создаст случайный пароль, удовлетворяющий политикам сложности пароля, значение которого необходимо ввести в поля «Пароль» и «Подтверждение».

Дополнительная кнопка  изменит скрытые символы на явные. Подтверждение пароля в этом случае не потребуется и соответствующее поле будет скрыто.

5. Далее необходимо нажать кнопку «Сохранить».
6. Для использования созданной учетной записи требуется ее активация (подробнее см. п. 5.1.4 «Активация и деактивация учетных записей»).
7. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

5.1.4 Активация и деактивация учетных записей

Активация учетных записей необходима для формирования списка учетных записей на клиентах.

Деактивация учетной записи необходима для временной приостановки использования учетной записи без ее удаления.

Чтобы активировать или деактивировать учетную запись необходимо поставить флаг напротив учетной записи либо убрать флаг соответственно. Затем необходимо нажать кнопку «Сохранить». Учетная запись будет активирована или деактивирована при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

 — отмеченное флагом поле означает, что данная учетная запись активна имеет доступ к выбранному объекту;

 — пустое поле означает, что учетная запись отключена для работы на выбранном

объекте.

5.1.4.1 Активация и деактивация учетных записей Windows

Активация и деактивация учетных записей Windows происходит в дереве «Агенты Windows». Далее необходимо выбрать уровень Сервера УД, либо уровень группы клиентов, либо уровень клиента и открыть вкладку «Учетные записи домена», либо «Учетные записи группы», либо «Учетные записи клиента» соответственно.

5.1.4.2 Активация и деактивация учетных записей vSphere

Активация и деактивация учетных записей vSphere происходит в дереве «Агенты ВИ» на уровне СВ во вкладке «Учетные записи» → «Учетные записи vSphere».

5.1.4.3 Активация и деактивация учетных записей vCSA

1. Активация и деактивация учетных записей vCSA происходит в дереве «Агенты ВИ» на уровне СВ во вкладке «Учетные записи» → «Учетные записи vSphere vCSA».

1.1. Активация и деактивация учетных записей локальной ОС vCSA для доступа к авторизации в ОС СВ vCSA локально или через SSH происходит в дереве «Агенты ВИ» на уровне СВ во вкладке «Учетные записи» → «Доступ к авторизации».

1.1.1. Для включения или отключения доступа к авторизации в SSO (Single Sign-On), а значит возможности работы через web-клиент и PowerCli, локальных учетных записей ОС vCSA нужно настроить членство в соответствующих группах vsphere.local[21] vCSA. Это происходит в дереве «Агенты ВИ» на уровне СВ во вкладке «Учетные записи» → «Группы vSphere vCSA».

1.1.2. Для активации всех учетных записей локальной ОС vCSA для доступа к авторизации в ОС СВ vCSA локально или через SSH, нужно перейти в дереве «Агенты ВИ» на уровне СВ на вкладку «Учетные записи» → «Доступ к авторизации» и нажать кнопку «Разблокировать всех» на панели «Действия».

1.2. Активация и деактивация учетных записей vCSA домена vsphere.local[21] для доступа к авторизации в SSO (Single Sign-On) (web-клиент или PowerCli) происходит в дереве «Агенты ВИ» на уровне СВ во вкладке «Учетные записи» → «Учетные записи vSphere vCSA».

1.2.1. Для включения или отключения доступа к авторизации в SSO (Single Sign-On), а значит возможности работы через web-клиент и PowerCli, учетных записей домена vsphere.local[21] vCSA нужно настроить членство в соответствующих группах vsphere.local[21] vCSA. Это происходит в дереве «Агенты ВИ» на уровне СВ во вкладке «Учетные записи» → «Группы vSphere vCSA».

Примечание. Важно понимать, что список пользователей «Учетные записи» → «Доступ к авторизации» содержит только пользователей локальной ОС vCSA (localos-пользователи), а список пользователей «Учетные записи» → «Учетные записи vSphere vCSA» содержит только пользователей домена vsphere.local[21]. Пользователи из этих двух списков не пересекаются!

Примечание. Для выдачи пользователю ОС (localos, с вкладки «Доступ к авторизации») прав для возможности работать с web-консолью управления или PowerCli (т.е. через SSO) необходимо включить его в группу Administrators, подробнее см. п. 5.2.2.1 «Управление группами домена vSphere». Однако это не приведет к тому, что данный пользователь появится в списке «Учетные записи» → «Учетные записи vSphere vCSA».

5.1.4.4 Активация и деактивация учетных записей гипервизора ESXi

Активация и деактивация учетных записей гипервизора происходит в дереве «Агенты ВИ» на уровне гипервизора во вкладке «Учетные записи» → «Учетные записи гипервизоров».

5.1.4.5 Активация и деактивация учетных записей гипервизора KVM

Активация и деактивация учетных записей гипервизора происходит в дереве «Агенты ВИ» на уровне гипервизора во вкладке «Системные учетные записи» → «Доступ к авторизации».

[21] Имя домена *vsphere.local* приводится в качестве примера, имя домена задается на этапе установки сервера виртуализации и может отличаться от указанного в руководстве.

5.1.4.6 Активация и деактивация учетных записей СВ oVirt/zVirt/HOSTVM/РЕД Вирт

Активация и деактивация учетных записей происходит в дереве «Агенты ВИ» на уровне СВ во вкладке «Учетные записи oVirt/zVirt/HOSTVM/РЕД Вирт» → «Учетные записи».

5.1.4.7 Активация и деактивация локальных учетных записей гипервизора/СВ oVirt/zVirt/HOSTVM/РЕД Вирт

Активация и деактивация учетных записей гипервизора происходит в дереве «Агенты ВИ» на уровне гипервизора/СВ во вкладке «Системные учетные записи» → «Доступ к авторизации».

5.1.5 Заблокированные пользователи

Учетная запись пользователя по разным причинам может быть заблокирована, например, вследствие неправильного ввода пароля несколько раз.

5.1.5.1 Разблокирование учетных записей клиентов Windows

Чтобы открыть список заблокированных пользователей на клиенте необходимо в дереве «Агенты Windows» перейти на уровень клиента и в категории «Состояние» нажать кнопку «Заблокированные пользователи» (рис. 141).

Примечание. Если кнопка «Заблокированные пользователи» неактивна, в категории «Действия» необходимо нажать кнопку  «Подключиться», либо выбрать соответствующий пункт из контекстного меню, чтобы осуществить оперативное подключение к клиенту.

В данном списке можно разблокировать выбранную учетную запись или несколько одновременно выделенных, нажав кнопку «Разблокировать» в блоке «Действия», и разблокировать все записи одновременно, нажав кнопку «Разблокировать всех» в блоке «Действия» либо выбрав пункт «Разблокировать пользователей» в контекстном меню.

Также разблокировать сразу все УЗ можно кнопкой «Разблокировать пользователей» (на уровне клиента вкладка «Состояние» → «Основное» → блок «Действия с клиентом») (см. п. 3.2.1.2 «Информационная панель клиента Windows»).

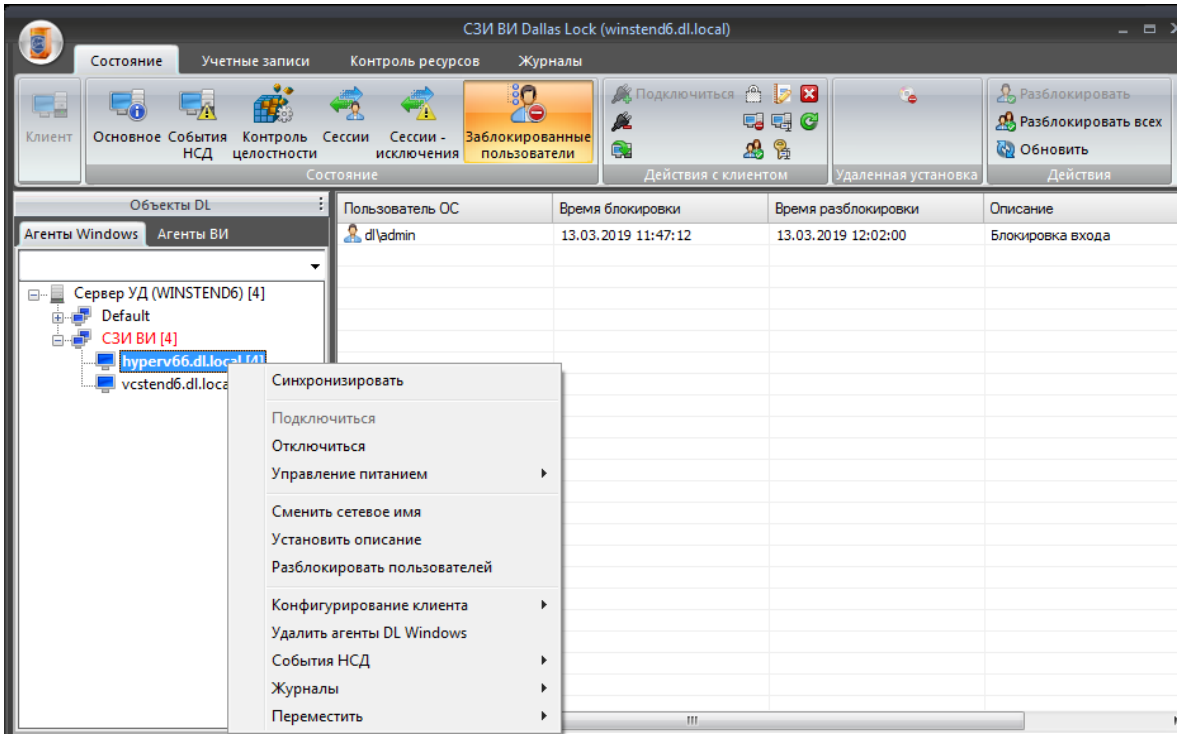


Рис. 141 – Действия со списком заблокированных пользователей

Внимание! Важно не путать данное свойство с параметром «отключена» учетной записи, не смотря на одинаковый запрет доступа к работе на ПК. Примером различного состояния заблокированных и отключенных учетных записей может быть следующий.

Под одной доменной учетной записью, зарегистрированной в СЗИ ВИ по маске, могут работать несколько доменных пользователей, и некоторые из них могут быть заблокированы, но в тоже время доменная учетная запись по маске не отключена. Учетные записи данных заблокированных пользователей будут отображаться в списке несмотря на то, что индивидуально в СЗИ ВИ они не зарегистрированы (зарегистрирована уч. запись по маске). В этом случае для разблокировки индивидуальных пользователей, для которых зарегистрирована одна на всех учетная доменная запись по маске, используется данная функция разблокировки в окне «Заблокированные пользователи».

5.1.5.2 Разблокирование учетных записей СВ vCSA

1) Для того, чтобы разблокировать учетную запись СВ после неудачной попытки локального входа необходимо:

1. Выбрать уровень СВ vCSA и открыть вкладку «Учетные записи».
2. Выбрать категорию «Доступ к авторизации».
3. Нажать кнопку «Разблокировать всех» в блоке действия.
4. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

2) Для того, чтобы разблокировать учетную запись СВ вследствие превышения числа попыток ввода пароля при авторизации через SSO (web-клиент или PowerCli) необходимо:

1. Выбрать уровень СВ vCSA и открыть вкладку «Учетные записи».
2. Выбрать категорию «Разблокировать доступ в web-клиент».
3. Выбрать учетную запись и нажать кнопку «Разблокировать» или «Разблокировать всех» в блоке действия.
4. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

5.1.5.3 Разблокирование учетных записей гипервизора ESXi

Для того, чтобы разблокировать учетную запись гипервизора необходимо:

1. Выбрать уровень гипервизора и открыть вкладку «Учетные записи».
2. Нажать кнопку «Разблокировать всех».
3. Нажать кнопку «Сохранить».
4. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

5.1.5.4 Разблокирование учетных записей гипервизора KVM

Для того, чтобы разблокировать учетную запись с правами доступа к авторизации на гипервизоре необходимо:

1. Выбрать уровень гипервизора и открыть вкладку «Учетные записи KVM».
2. Выбрать категорию «Доступ к авторизации».
3. Нажать кнопку «Разблокировать всех».
4. Нажать кнопку «Сохранить».
5. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

5.1.5.5 Разблокирование учетных записей СВ oVirt/zVirt/HOSTVM/РЕД Вирт

Для того, чтобы разблокировать учетную запись СВ вследствие превышения числа попыток ввода пароля при авторизации через web-клиент необходимо:

1. Выбрать уровень СВ и открыть вкладку «Учетные записи oVirt/zVirt/HOSTVM/РЕД Вирт».
2. Выбрать категорию «Учетные записи».
3. Нажать кнопку «Разблокировать всех».
4. Нажать кнопку «Сохранить».
5. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

5.1.5.6 Разблокирование локальных учетных записей СВ/гипервизора

oVirt/zVirt/HOSTVM/РЕД Вирт

Для того, чтобы разблокировать учетную запись с правами доступа к авторизации на гипервизоре/СВ необходимо:

1. Выбрать уровень гипервизора/СВ и открыть вкладку «Системные учетные записи».
2. Выбрать категорию «Доступ к авторизации».
3. Нажать кнопку «Разблокировать всех».
4. Нажать кнопку «Сохранить».
5. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

5.1.6 Удаление учетных записей

Для удаления учетной записи из ВИ вне зависимости от того, какими средствами она создана или зарегистрирована в самой системе защиты, необходимо выделить ее имя в списке главного окна программы, нажать кнопку «Удалить» или выбрать соответствующее действие из контекстного меню. Подтвердить операцию, после чего синхронизировать, открыв вкладку «Состояние» и нажав кнопку «Синхронизировать». Учетная запись будет удалена из ЦУ СЗИ ВИ и из самого Сервера виртуализации.

Следует отметить, что при удалении самой СЗИ ВИ, учетные записи, созданные средствами ЦУ СЗИ ВИ, остаются на сервере виртуализации.

Внимание! При появлении ошибки синхронизации, связанной с невозможностью применения права на отсутствующего пользователя для прекращения вывода сообщения об ошибке необходимо либо активировать данного пользователя на указанном узле, либо исключить у данного пользователя на данном узле наличие права, которое устанавливается на этого пользователя.

5.1.7 Смена пароля

В некоторых ситуациях, например, когда пользователь забыл свой пароль, администратору бывает необходимо задать пользователю новый пароль, не зная старого. Для это необходимо:

1. Открыть одну из категорий для редактирования учетных записей
   - Для УЗ vSphere - в дереве «Агенты ВИ» на уровне группы vSphere → «Учетные записи vSphere»;
   - Для УЗ KVM - в дереве «Агенты ВИ» на уровне гипервизора KVM → «Системные учетные записи»;
   - Для УЗ oVirt/zVirt/HOSTVM/РЕД Вирт - в дереве «Агенты ВИ» на уровне СВ oVirt/zVirt/HOSTVM/РЕД Вирт → «Учетные записи oVirt/zVirt/HOSTVM/РЕД Вирт»;
   - Для локальных УЗ oVirt/zVirt/HOSTVM - в дереве «Агенты ВИ» на уровне СВ/гипервизора oVirt/zVirt/HOSTVM/РЕД Вирт → «Системные учетные записи»;
   - Для УЗ Windows - в дереве «Агенты Windows» на уровне Сервера УД → «Учетные записи домена», либо на уровне клиента → «Учетные записи»).
2. Выбрать учетную запись в списке и нажать кнопку «Задать пароль» в блоке «Действия».
3. Далее следует назначить пароль, который соответствует заданным парольным политикам и нажать кнопку «ОК».

   При вводе пароля необходимо руководствоваться следующими правилами:

   - максимальная длина пароля 32 символа;
   - пароль может содержать латинские символы, символы кириллицы, цифры и специальные символы (список допустимых символов см. в описании политики безопасности «[Сервер виртуализации] Пароли: минимальное количество специальных символов» в п.5.3 «Настройки параметров безопасности для объектов ВИ»);
   - сложность пароля (наличие определенных символов, длина, срок действия и прочие) регулируется специальными политиками безопасности, которые устанавливаются администратором (см. п.5.3 «Настройки параметров безопасности для объектов ВИ»).

   Для создания пароля, отвечающего всем установленным требованиям политик безопасности, можно воспользоваться помощью генератора паролей системы защиты. Для этого нажать кнопку «Генерация пароля». Система автоматически создаст случайный пароль, удовлетворяющий политикам сложности пароля, значение которого необходимо ввести в поля «Пароль» и «Подтверждение».

Дополнительная кнопка  изменит скрытые символы на явные. Подтверждение пароля в этом случае не потребуется и соответствующее поле будет скрыто. В случае корректного ввода нового пароля появится сообщение об успешной смене пароля.

4. Открыть вкладку «Состояние» и нажать кнопку «Синхронизировать».

Примечание. При изменении пароля администратора СВ vSphere/ oVirt/zVirt/HOSTVM/РЕД Вирт или гипервизора ESXi/KVM/oVirt/zVirt/HOSTVM/РЕД Вирт штатными средствами, учетные данные которого были установлены при подключении к СЗИ ВИ, необходимо выполнить повторную установку учетных данных (см. п. 2.7.1 «Установка учетных данных для vSphere», п. 2.7.2 «Установка учетных данных для гипервизора KVM», п. 2.7.3 «Установка учетных данных для СВ »).

5.2 Управление группами пользователей

Группы предназначены для объединения пользователей со схожими правами безопасности. Такое объединение может упростить работу администратора, при выполнении настроек СЗИ ВИ.

Группы упрощают управление Сервером виртуализации. Можно добавлять пользователей к группам и назначать этим группам определенную роль, удалять пользователей из групп в соответствии с потребностями этих пользователей.

5.2.1 Управление группами пользователей клиентов Windows

5.2.1.1 Создание групп Windows

Для создания новой группы Windows необходимо:

1. Открыть дерево «Агенты Windows».
2. Выбрать уровень «Сервера УД» и открыть категорию «Учетные записи домена» → «Группы» (рис. 142).

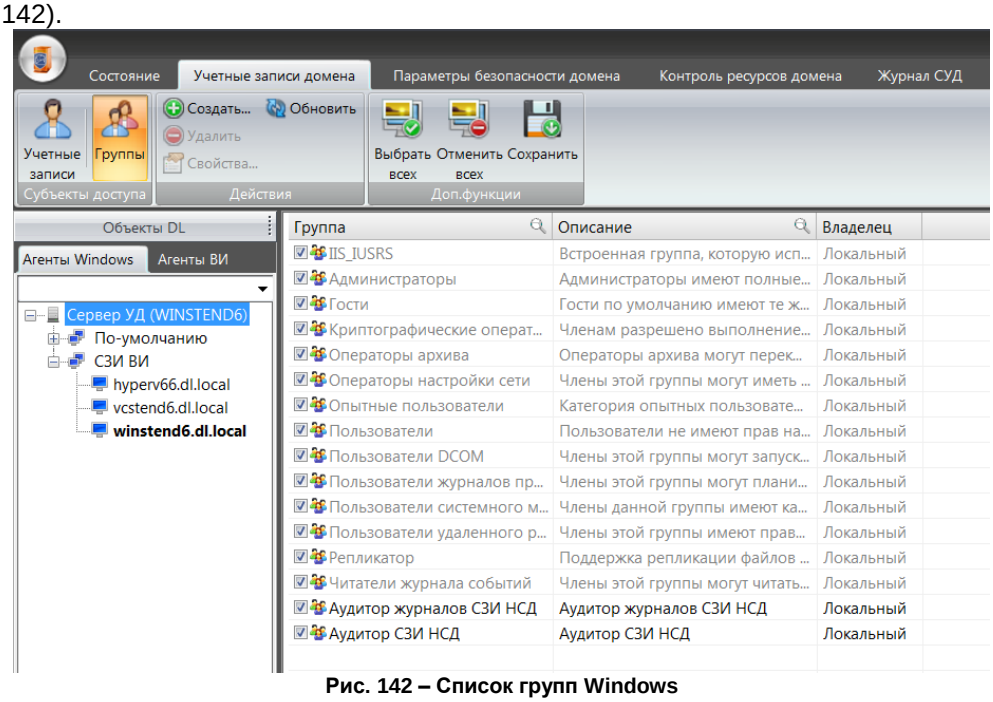


Рис. 142 – Список групп Windows

3. Нажать кнопку «Создать».
4. В появившемся окне ввести имя группы и заполнить поле «Описание» при необходимости, после чего нажать кнопку «ОК» (рис. 143).

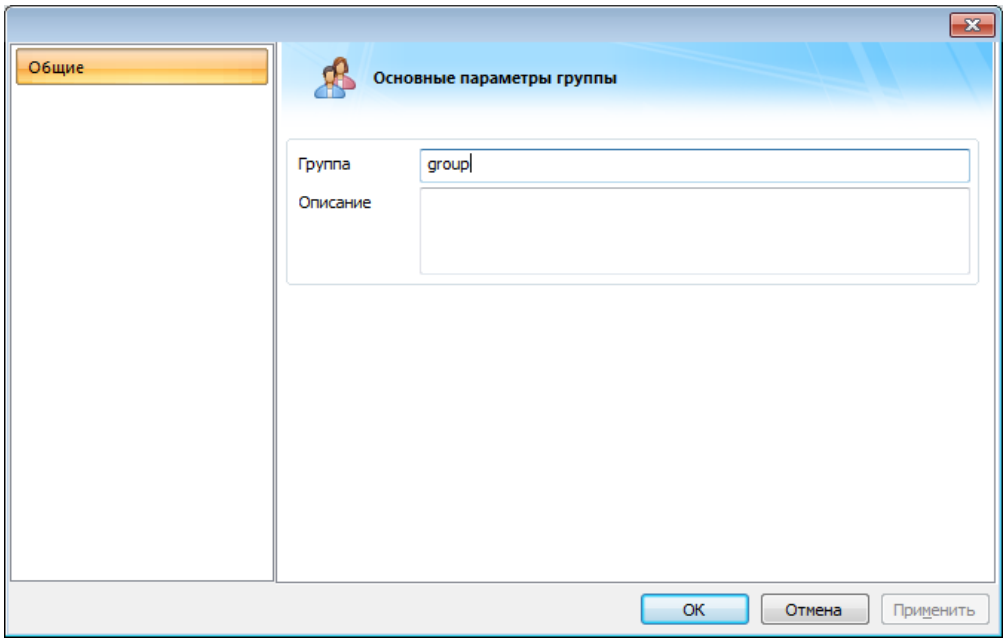


Рис. 143 – Окно создания новой группы

Изменить описание группы можно, используя кнопку «Свойства» или выбрав данное действие из контекстного меню.

Назначить все необходимые политики безопасности для созданной группы можно, редактируя параметры безопасности различных категорий параметров.

5.2.1.2 Активация и деактивация групп пользователей

Чтобы активировать или деактивировать группу необходимо в поле напротив нее установить, либо убрать флаг соответственно. Затем необходимо нажать кнопку «Сохранить». Группа будет активирована или деактивирована при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

Внимание! Деактивация группы при следующей синхронизации приводит к удалению группы на клиенте Windows, но с сохранением имени группы в списке СЗИ ВИ.

5.2.2 Управление группами пользователей ВИ

5.2.2.1 Управление группами домена vSphere

Создание групп vCenter

Для создания новой группы vCenter необходимо:

1. Выбрать уровень СВ vCenter и открыть категорию «Учетные записи» → «Группы vSphere» (рис. 144).

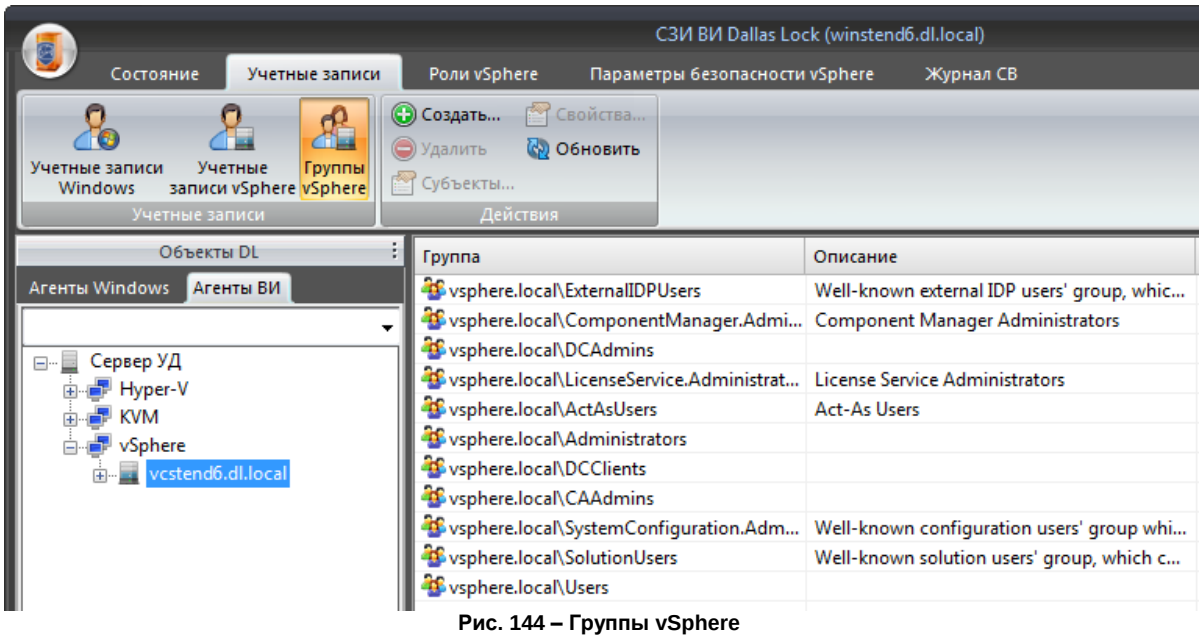


Рис. 144 – Группы vSphere

2. В категории действия нажать кнопку «Создать».
3. В появившемся окне ввести имя группы и выбрать домен. Далее при необходимости заполнить поле «Описание» и добавить субъекты группы (см. ниже).
4. Завершить процесс создания группы, нажав кнопку «ОК» (рис. 145).

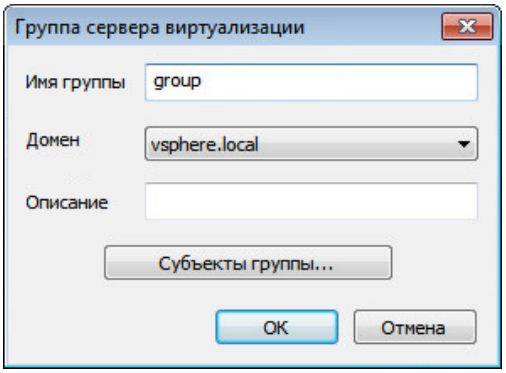


Рис. 145 – Окно создания новой группы

5. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

Создание групп vCSA

Для создания новой группы vCSA необходимо:

1. Выбрать уровень СВ (vCSA) и открыть категорию «Учетные записи» → «Группы vSphere vCSA» (рис. 146).

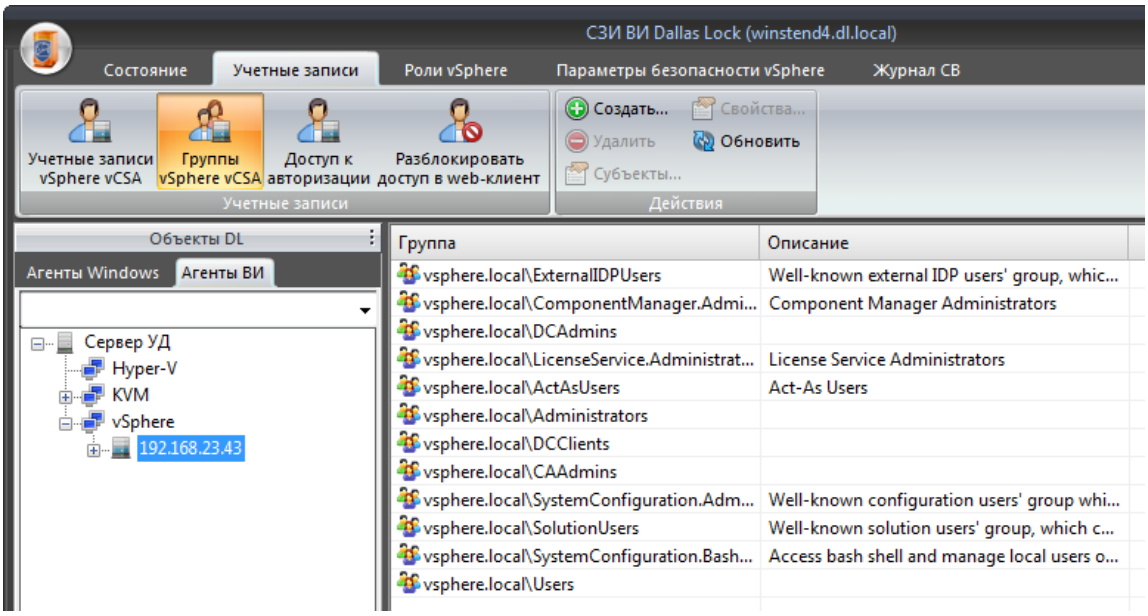


Рис. 146 – Группы vCSA

2. В категории действия нажать кнопку «Создать».
3. В появившемся окне ввести имя группы и выбрать домен. Далее при необходимости заполнить поле «Описание» и добавить субъекты группы.
4. Завершить процесс создания группы, нажав кнопку «ОК».
5. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

Добавление пользователя в группу

Чтобы добавить пользователя в группу необходимо:

1. Выделить группу и нажать кнопку «Субъекты…» в блоке «Действия» или в процессе создания группы нажать кнопку «Субъекты группы…».
2. В обоих случаях появится окно редактирования членов группы vsphere.local (рис. 147).

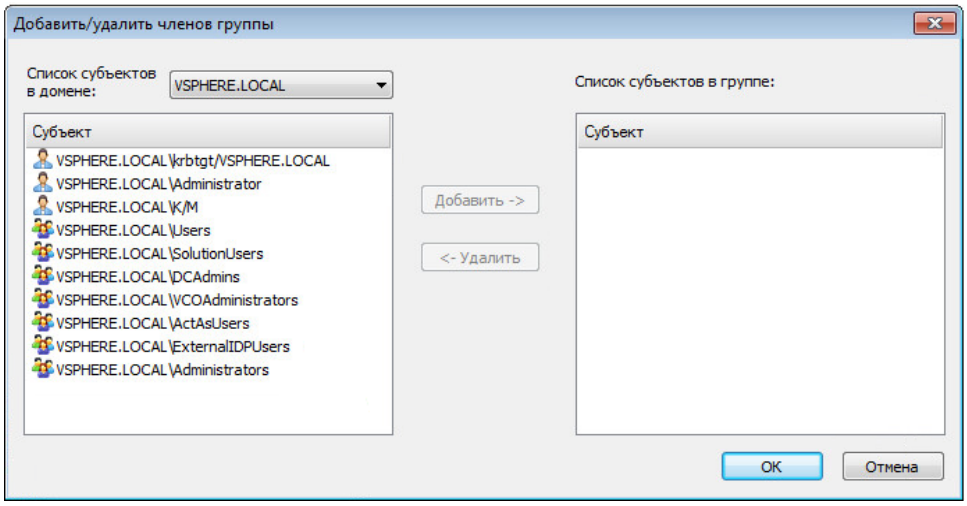


Рис. 147 – Окно редактирования членов группы

3. В выпадающем списке параметра «Список субъектов в домене» при необходимости выбрать другой домен.

Примечание. При добавлении локального пользователя Windows в список субъектов группы vsphere данный пользователь должен быть синхронизирован на Сервере виртуализации (vCenter).

4. Выделить субъект в левом списке «Список субъектов в домене» и нажать кнопку «Добавить», после чего данный субъект будет перемещен в правый список «Список субъектов в группе» (рис. 148).

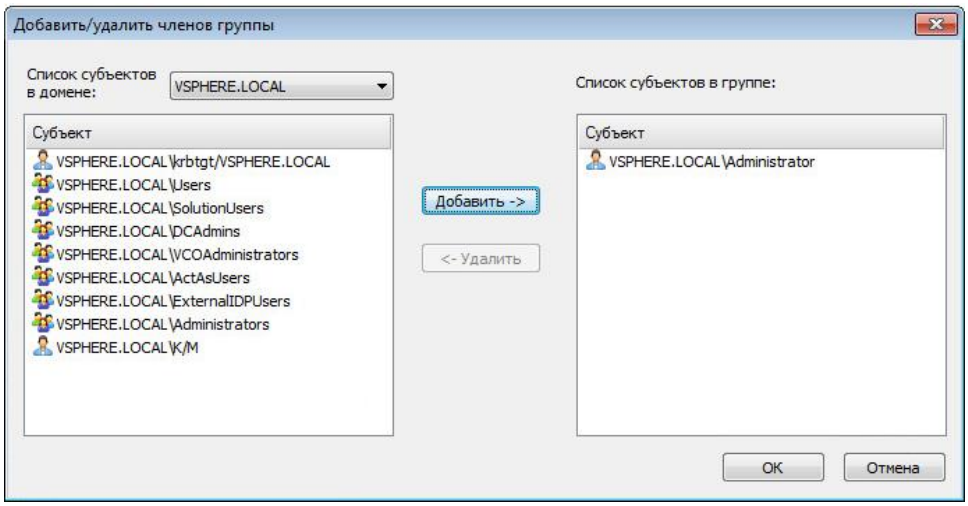


Рис. 148 – Окно редактирования членов группы vsphere.local

5. Чтобы удалить субъект, необходимо выделить его в «Списке субъектов в группе» и нажать кнопку «Удалить», соответственно (рис. 149).

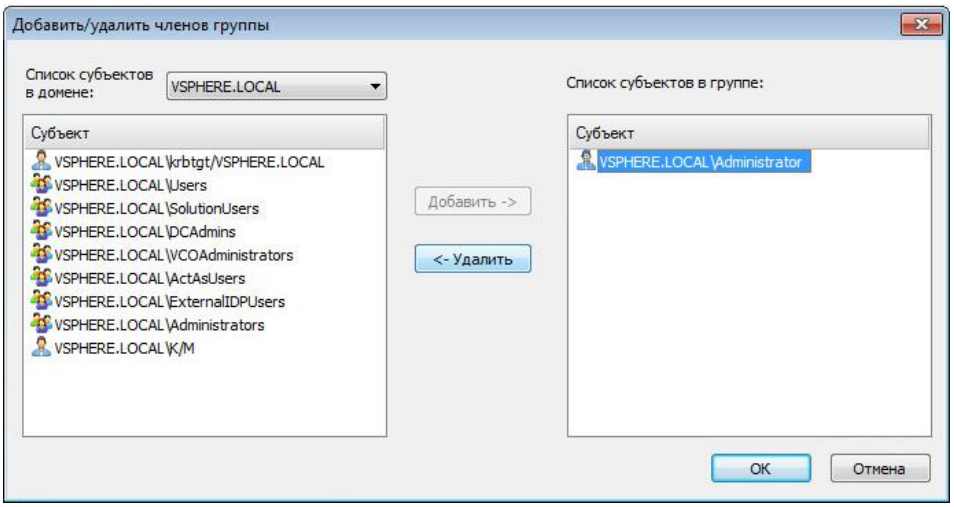


Рис. 149 – Окно редактирования членов группы vsphere.local

6. После завершения редактирования субъектов группы нажать кнопку «ОК».

5.2.2.2 Управление группами гипервизора KVM

Создание группы KVM

Для создания новой группы KVM необходимо:

1. Выбрать уровень гипервизора KVM и открыть вкладку «Учетные записи KVM» → «Группы» (рис. 150).

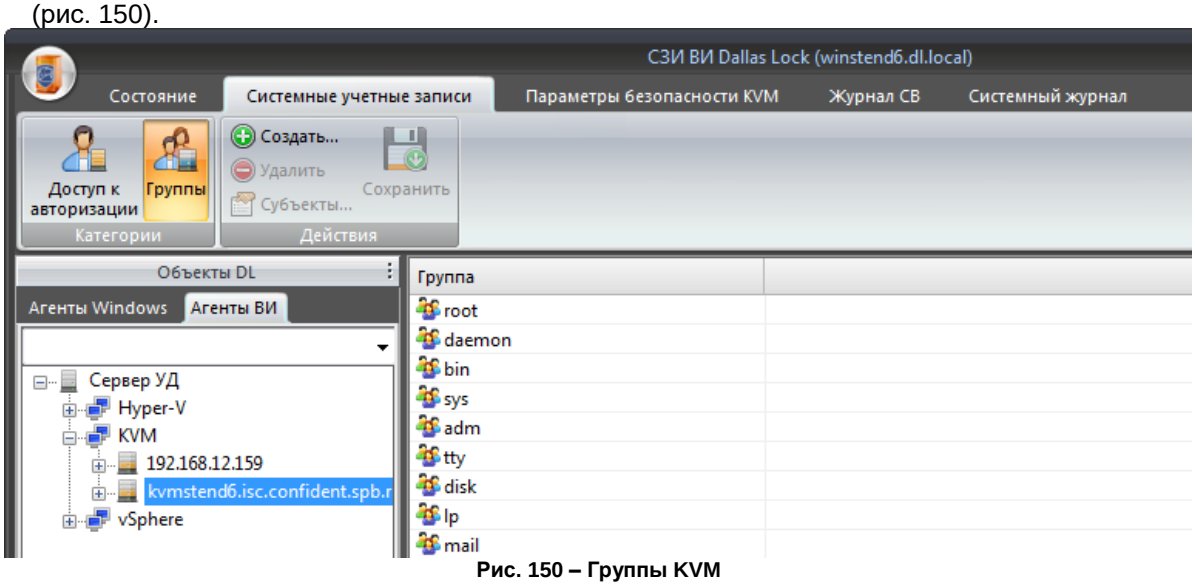


Рис. 150 – Группы KVM

2. Нажать кнопку «Создать».
3. В появившемся окне ввести имя группы (рис. 151).

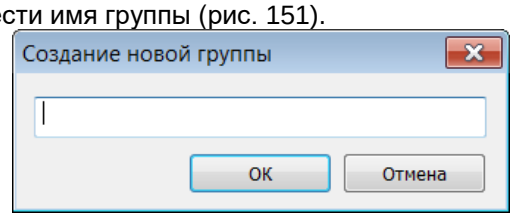


Рис. 151 – Окно создания новой группы KVM

4. Завершить процесс создания группы, нажав кнопку «ОК».
5. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

Добавление пользователя в группу KVM

Чтобы добавить пользователя в группу необходимо:

1. Выделить группу и нажать кнопку «Субъекты…» в блоке «Действия» или выбрать соответствующий пункт в контекстном меню.
2. В появившемся окне выделить субъект в левом списке «Список субъектов» и нажать кнопку «Добавить», после чего данный субъект будет перемещен в правый список «Список субъектов в группе» (рис. 152).

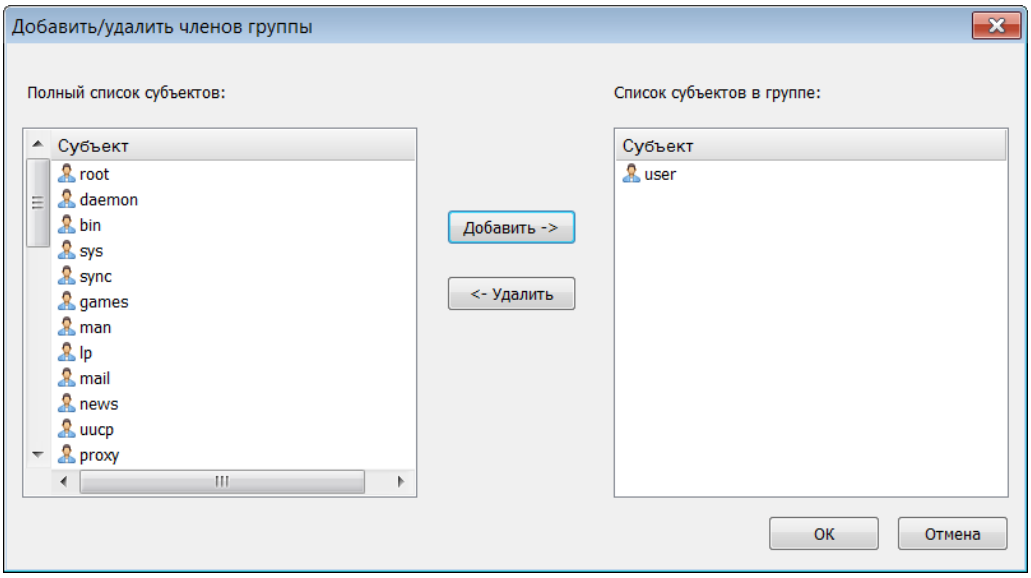


Рис. 152 – Окно редактирования членов группы

3. Чтобы удалить субъект, необходимо выделить его в «Списке субъектов в группе» и нажать кнопку «Удалить», соответственно.
4. После завершения редактирования субъектов группы нажать кнопку «ОК».
5. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

5.2.2.3 Управление группами oVirt/zVirt/HOSTVM/РЕД Вирт

Создание группы СВ о oVirt/zVirt/HOSTVM/РЕД Вирт

Для создания новой группы oVirt/zVirt/HOSTVM/РЕД Вирт необходимо:

1. Выбрать уровень СВ oVirt/zVirt/HOSTVM/РЕД Вирт и открыть вкладку «Учетные записи oVirt/zVirt/HOSTVM/РЕД Вирт» → «Группы» (рис. 153).

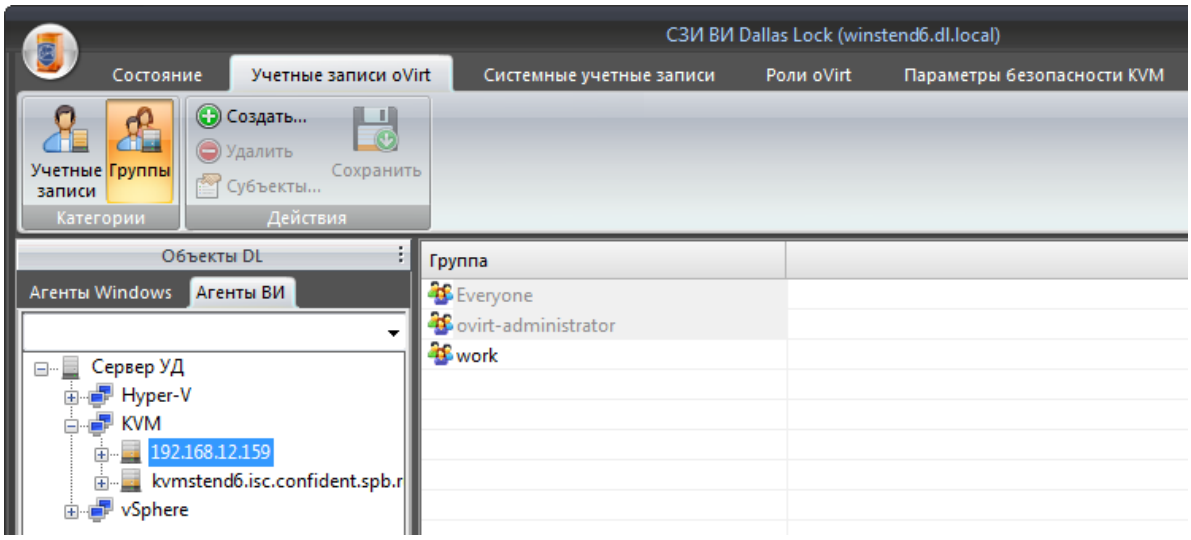


Рис. 153 – Группы oVirt/zVirt/HOSTVM/РЕД Вирт

2. Нажать кнопку «Создать».
3. В появившемся окне ввести имя группы (рис. 154).

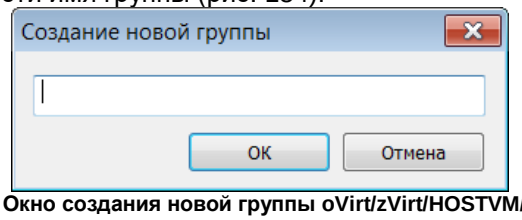


Рис. 154 – Окно создания новой группы oVirt/zVirt/HOSTVM/РЕД Вирт

4. Завершить процесс создания группы, нажав кнопку «ОК».
5. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»)

Создание локальной группы гипервизора/СВ oVirt/zVirt/HOSTVM/РЕД Вирт

Для создания новой локальной группы oVirt/zVirt/HOSTVM/РЕД Вирт необходимо:

6. Выбрать уровень гипервизора/СВ oVirt/zVirt/HOSTVM/РЕД Вирт и открыть вкладку «Системные учетные записи» → «Группы» (рис. 155).

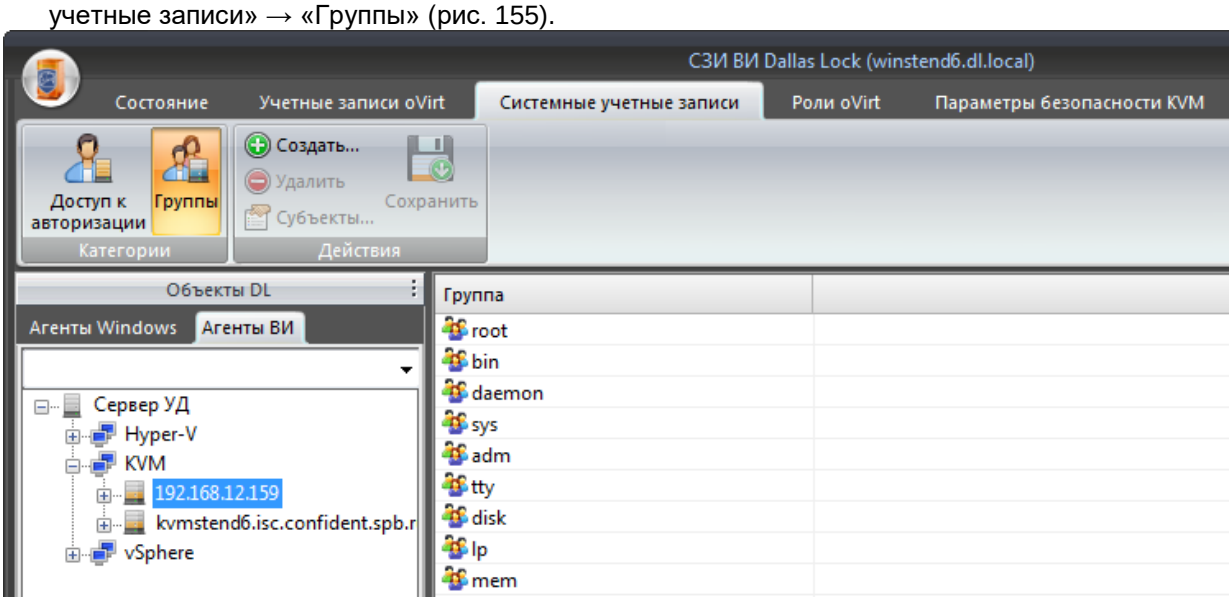


Рис. 155 – Локальные группы oVirt/zVirt/HOSTVM/РЕД Вирт

7. Нажать кнопку «Создать».
8. В появившемся окне ввести имя группы (рис. 156).

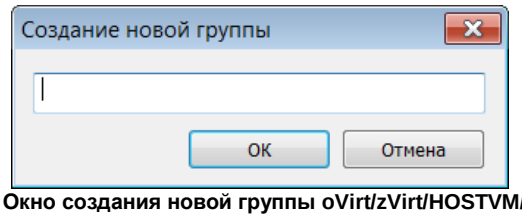


Рис. 156 – Окно создания новой группы oVirt/zVirt/HOSTVM/РЕД Вирт

9. Завершить процесс создания группы, нажав кнопку «ОК».
10. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

Добавление пользователя в группу oVirt/zVirt/HOSTVM/РЕД Вирт

Чтобы добавить пользователя в группу необходимо:

1. Выделить группу и нажать кнопку «Субъекты…» в блоке «Действия» или выбрать соответствующий пункт в контекстном меню.
2. В появившемся окне выделить субъект в левом списке «Список субъектов» и нажать кнопку «Добавить», после чего данный субъект будет перемещен в правый список «Список субъектов в группе» (рис. 152).

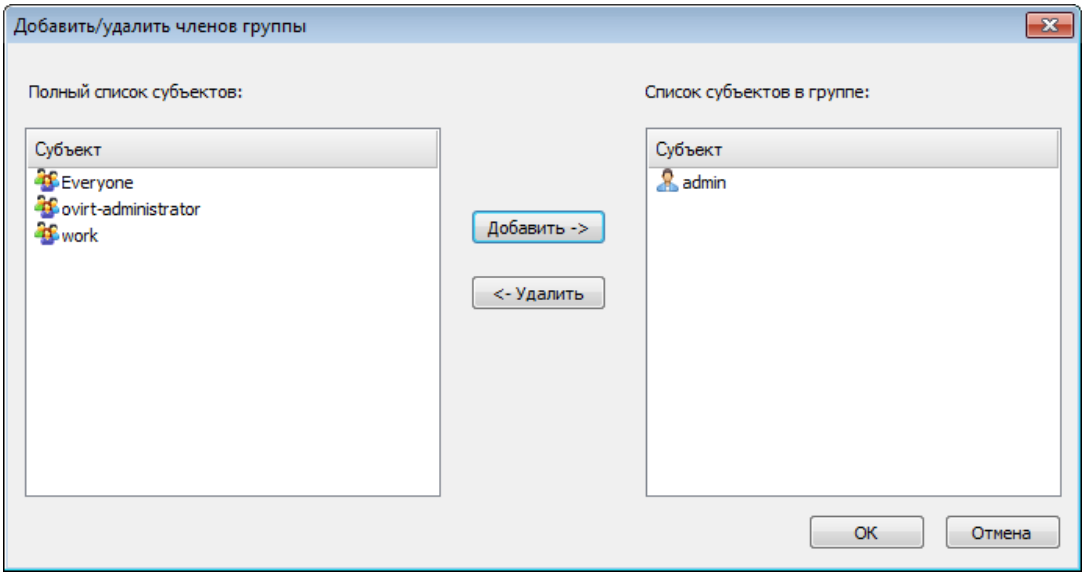


Рис. 157 – Окно редактирования членов группы

3. Чтобы удалить субъект, необходимо выделить его в «Списке субъектов в группе» и нажать кнопку «Удалить», соответственно.
4. После завершения редактирования субъектов группы нажать кнопку «ОК».
5. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

5.2.3 Удаление группы

Для удаления группы необходимо выделить соответствующую группу, нажать кнопку «Удалить» или выбрать данное действие в контекстном меню. На экране отобразится подтверждение на удаление. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

5.3 Настройки параметров безопасности для объектов ВИ

5.3.1 Настройки параметров безопасности

5.3.1.1 Параметры входа для vSphere

Просмотр и редактирование параметров входа для объектов ВИ vSphere происходит на уровне vSphere в категории «Параметры безопасности vSphere» → «Вход» (рис. 158).

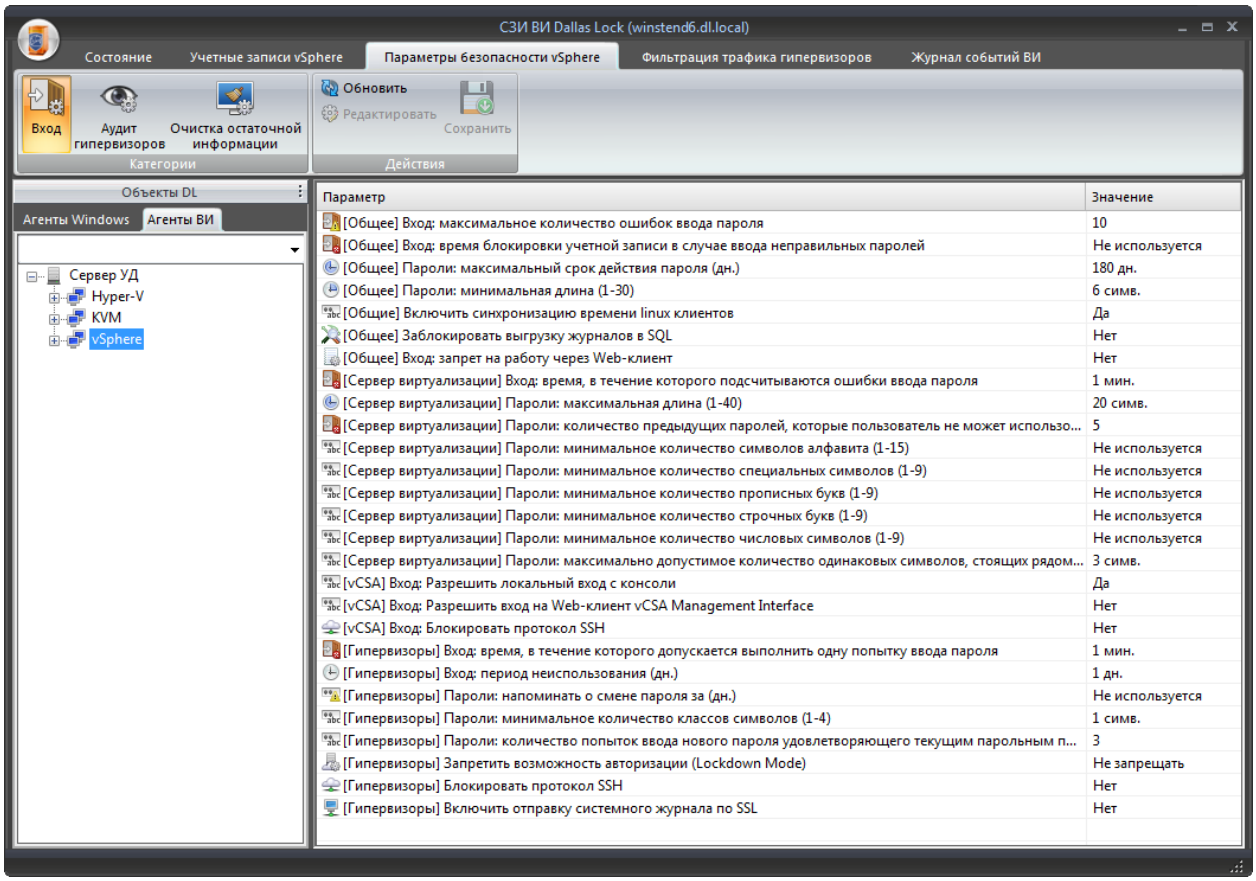


Рис. 158 – Параметры входа vSphere

Данные параметры входа применимы только для сервера виртуализации и гипервизора.

[Общее] Вход: максимальное количество ошибок ввода пароля

Значение, установленное для этого параметра, регламентирует, сколько раз пользователь имеет право ошибаться при вводе пароля. По умолчанию данное значение равно 10.

Если при входе на сервер виртуализации или гипервизор пользователь вводит неверный пароль и число ошибок превысит больше допустимого, учетная запись будет заблокирована. Сбросить автоматическую блокировку досрочно может только администратор безопасности или пользователь, обладающий правом редактирования учетных записей.

[Общее] Вход: время блокировки учетной записи в случае ввода неправильных паролей

Данный параметр позволяет установить, сколько времени учетная запись будет заблокирована после того, как пользователь ввел неверный пароль больше допустимого числа раз.

По истечении указанного времени учетная запись автоматически разблокируется, и пользователь снова получит возможность ввести пароль.

Значение «Не используется», установленное по умолчанию, указывает на то, что срок блокировки будет бессрочный.

Примечание. Данная политика работает применительно к учетным записям, принадлежащим домену vsphere.local.

Примечание. Значение данной политики определяется в диапазоне от «не используется» (0 секунд) до «5 часов» (18000 секунд). Значение одноименной политики на хосте ESXi, наследуемой от данной, ограничено реализацией платформы ESXi интервалом от 1 до 3600 секунд, при синхронизации политик vSphere и ESXi итоговые значения будут заданы согласно таблице:

№	Значение политики vSphere	Значение политики ESXi
1	«Не используется»	1 секунда

2	От 1 минуты до 60 минут	равно значению политики vSphere
3	Более 60 минут	3600 секунд (60 минут)

[Общее] Пароли: максимальный срок действия пароля (дн.)

Данным параметром устанавливается максимальный срок действия пароля для всех пользователей. По истечении установленного срока, пользователь должен сменить пароль при входе на сервер виртуализации или гипервизор. Если выбрано значение «Не используется», то время действия пароля не ограничено.

По умолчанию значение данного параметра: 180 дн.

[Общее] Пароли: минимальная длина

Данным параметром устанавливается ограничение на минимальную длину пароля.

При регистрации новой учетной записи и при изменении старого пароля СЗИ ВИ DL контролирует длину вводимого пароля. Если число символов в пароле меньше установленного значения, то на экране появится предупреждение «Ввод пароля: введен слишком короткий пароль».

Следует иметь в виду, что если в процессе работы изменить значение длины пароля (например, увеличить), то у зарегистрированных учетных записей она останется прежней до первой смены пароля.

По умолчанию значение данного параметра: 6 симв.

[Общее] Заблокировать выгрузку журналов в SQL

Данный параметр позволяет блокировать выгрузку журналов syslog в SQL, для предотвращения передачи служебных данных.

По умолчанию значение данного параметра: «Нет».

[Общее] Вход: запрет на работу через Web-клиент

Данный параметр позволяет заблокировать возможность подключения к серверу виртуализации или гипервизору ESXi через Web-клиент VMware vSphere.

По умолчанию значение данного параметра: «Нет».

[Общие] Включить синхронизацию времени linux клиентов

Данный параметр позволяет отключить синхронизацию времени между СЗИ ВИ и гипервизорами, работающими на ОС семейства Linux.

По умолчанию значение данного параметра «Да».

[Сервер виртуализации] Вход: время, в течение которого подсчитываются ошибки ввода пароля (мин.)

Данный параметр позволяет установить количество времени, в течение которого подсчитываются ошибки ввода пароля. Если за данный период времени количество неудачных попыток входа достигнет максимального количества ошибок ввода пароля, учетная запись будет заблокирована на время, заданное в параметре «[Общее] Вход: время блокировки учетной записи в случае ввода неправильных паролей».

В случае, если за установленное время количество неудачных попыток входа не достигло заданного максимального количества ошибок ввода пароля – счетчик неудачных попыток обнуляется.

По умолчанию значение данного параметра: 1 мин.

[Сервер виртуализации] Пароли: максимальная длина (1-40)

Данным параметром устанавливается ограничение на максимальную длину пароля.

По умолчанию значение данного параметра: 20 символов.

[Сервер виртуализации] Пароли: количество предыдущих паролей, которые пользователь не может использовать

Данным параметром устанавливается количество предыдущих паролей каждого пользователя, которые не могут быть выбраны ими при смене пароля. Например, значение «5», установленное по умолчанию, запрещает использовать пять предыдущих паролей для выбранного пользователя.

[Сервер виртуализации] Пароли: минимальное количество символов алфавита

Данным параметром устанавливается минимальное количество символов алфавита, которые должны присутствовать при задании пароля, для учетной записи Сервера виртуализации.

По умолчанию значение данного параметра: «Не используется».

[Сервер виртуализации] Пароли: минимальное количество специальных символов

Данным параметром устанавливается минимальное количество специальных символов («`», «~», «!», «@», «#», «$», «%», «^», «&», «*», «(», «)», «_», «-», «+», «{», «}», «[», «]», «\», «|», «:», «;», ««», «'», «<», «>», «,», «.», «?», «/»), которые должны присутствовать при задании пароля, для учетной записи Сервера виртуализации.

По умолчанию значение данного параметра: «Не используется».

[Сервер виртуализации] Пароли: минимальное количество прописных букв

Данным параметром устанавливается минимальное количество прописных (больших) букв, которые должны присутствовать при задании пароля, для учетной записи Сервера виртуализации.

По умолчанию значение данного параметра: «Не используется».

[Сервер виртуализации] Пароли: минимальное количество строчных букв

Данным параметром устанавливается минимальное количество строчных (маленьких) букв, которые должны присутствовать при задании, для учетной записи Сервера виртуализации.

По умолчанию значение данного параметра: «Не используется».

[Сервер виртуализации] Пароли: минимальное количество числовых символов

Данным параметром устанавливается минимальное количество строчных (маленьких) букв, которые должны присутствовать при задании пароля, для учетной записи Сервера виртуализации.

По умолчанию значение данного параметра: «Не используется».

[Сервер виртуализации] Пароли: максимально допустимое количество одинаковых символов, стоящих рядом

Данным параметром устанавливается максимально допустимое количество одинаковых символов, которые могут присутствовать при задании пароля, для учетной записи Сервера виртуализации.

По умолчанию значение данного параметра: 3 симв.

[VCSA] Вход: Разрешить локальный вход с консоли

Данный параметр позволяет настроить разрешение локального входа с консоли.

По умолчанию значение данного параметра: «Да».

[VCSA] Вход: Разрешить вход на Web-клиент VCSA Management Interface

Данный параметр позволяет настроить разрешение входа на Web-клиент VCSA Management Interface.

По умолчанию значение данного параметра: «Нет».

[VCSA] Вход: Блокировать протокол SSH

Параметр контролирует удаленный доступ в vCSA по протоколу SSH.

По умолчанию значение данного параметра: «Нет».

[Гипервизоры] Вход: время, в течение которого допускается выполнить одну попытку ввода пароля (мин.)

Данный параметр позволяет установить, количество времени в течение которого допускается выполнить одну попытку ввода пароля. Если произошла неудачная попытка ввода пароля, то выполнить новую попытку ввода пароля возможно будет только через указанный период времени.

По умолчанию значение данного параметра: 1 мин.

[Гипервизоры] Вход: период неиспользования (дн.)

Данным параметром устанавливается период времени, через который будут отключены неиспользуемые учетные записи гипервизора. Сбросить автоматическую блокировку досрочно может только администратор безопасности или пользователь, обладающий правом редактирования учетных записей.

По умолчанию значение данного параметра: «Не используется».

[Гипервизоры] Пароли: напоминать о смене пароля за (дн.)

С помощью данного параметра СЗИ ВИ позволит напоминать пользователю о том, что через

определенное количество дней необходимо сменить пароль. Напоминание о предстоящей смене пароля будет появляться на экране при загрузке ОС данным пользователем, начиная с того момента, когда до смены пароля (фактически до истечения максимального времени действия пароля) осталось количество дней, равное установленному значению для этой политики. По умолчанию значение данного параметра: «Не используется».
[Гипервизоры] Пароли: минимальное количество классов символов (1-4)
Данный параметр определяет количество классов символов (буквы в верхнем и нижнем регистре, цифры и специальные символы), которые должны присутствовать в пароле. Этот параметр может принимать значения от 1 до 4. Значение «1» означает, что пароль может содержать любые символы, например, только цифры. По умолчанию значение данного параметра: 3 симв.
[Гипервизоры] Вход: количество попыток ввода нового пароля, удовлетворяющего текущим парольным политикам
Значение, установленное для этого параметра, регламентирует, сколько раз пользователь имеет право ошибаться при вводе нового пароля. По умолчанию значение данного параметра: 3.
Запретить возможность авторизации (Lockdown Mode)
Данный параметр позволяет настроить запрет возможности авторизации. Возможно установить запрет при удаленном подключении, при прямом и удаленном подключении. По умолчанию значение данного параметра: «Не запрещать».
[Гипервизоры] Блокировать протокол SSH
Если разрешено использование ESXi Shell, то его можно запустить непосредственно на гипервизоре ESXi через DCUI или удаленно по SSH. Данный параметр блокирует такую возможность. По умолчанию значение данного параметра: «Нет».
[Гипервизоры] Включить отправку системного журнала по SSL
Данный параметр позволяет включать шифрование информации, передаваемой по протоколу syslog. По умолчанию значение данного параметра: «Нет».

Примечание. Данная политика работает только с добавленным корневым сертификатом СЗИ ВИ в доверенные корневые сертификаты VMware PSC (подробнее см. Приложение № 2. «Добавление корневого сертификата СЗИ ВИ в доверенные корневые сертификаты VMware PSC».)

5.3.1.2 Параметры входа для Hyper-V

Просмотр и редактирование параметров входа для объектов ВИ Hyper-V происходит в дереве «Агенты Windows» на уровне Сервера УД в категории «Параметры безопасности домена» → «Вход». Подробное описание приведено в п. 5.4.3 «Настройка параметров ».

5.3.1.3 Параметры входа для KVM/oVirt/zVirt/HOSTVM/РЕД Вирт

Просмотр и редактирование параметров входа для объектов ВИ KVM происходит в дереве «Агенты ВИ» на уровне KVM в категории «Параметры безопасности KVM» → «Вход» (рис. 159).

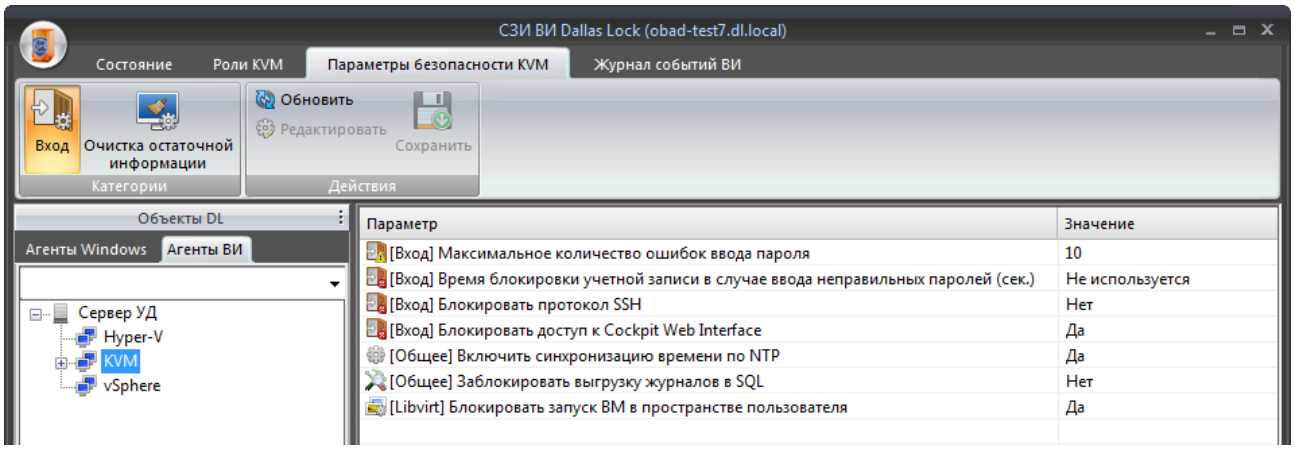


Рис. 159 – Параметры входа KVM

Данные параметры входа применимы только для сервера виртуализации и гипервизора.

Вход: максимальное количество ошибок ввода пароля

Значение, установленное для этого параметра, регламентирует, сколько раз пользователь имеет право ошибаться при вводе пароля. По умолчанию данное значение равно 10.

Если при входе на сервер виртуализации или гипервизор пользователь вводит неверный пароль и число ошибок превысит больше допустимого, учетная запись будет заблокирована. Сбросить автоматическую блокировку досрочно может только администратор безопасности или пользователь, обладающий правом редактирования учетных записей.

Вход: время блокировки учетной записи в случае ввода неправильных паролей (сек.)

Данный параметр позволяет установить, сколько времени учетная запись будет заблокирована после того, как пользователь ввел неверный пароль больше допустимого числа раз.

По истечении указанного времени учетная запись автоматически разблокируется, и пользователь снова получит возможность ввести пароль.

Значение «Не используется», установленное по умолчанию, указывает на то, что срок блокировки будет бессрочный.

Вход: блокировать протокол SSH

Данный параметр блокирует удаленный доступ к СВ по протоколу SSH.

По умолчанию значение данного параметра: «Да».

Примечание. Для возможности удаленного подключения к клиенту по протоколу SSH помимо отключения данной политики необходимо добавить компьютер, с которого будет осуществляться подключение, в список клиентов управления СВ (подробнее см. п.6.3.2.3 «Клиенты управления СВ KVM/oVirt/zVirt/HOSTVM»)

Вход: блокировать доступ к Cockpit Web Interface

Данный параметр позволяет настроить разрешение входа на Web-клиент Cockpit Web Interface.

По умолчанию значение данного параметра: «Да».

Общее: Включить синхронизацию времени по NTP

Данный параметр позволяет использовать NTP-сервера из заданного списка для синхронизации времени между сервером УД и агентами СЗИ ВИ.

По умолчанию значение данного параметра: «Да».

Общее: Заблокировать выгрузку журналов в SQL

Данный параметр позволяет блокировать выгрузку журналов syslog в SQL, для предотвращения передачи служебных данных.

По умолчанию значение данного параметра: «Нет».

Libvirt: Блокировать запуск ВМ в пространстве пользователя

Данный параметр позволяет блокировать запуск ВМ в пространстве пользователя, т.е. работа с ВМ может выполнятся только для root-пользователя.

По умолчанию значение данного параметра: «Да».

5.4 Настройки параметров для клиентов Windows

5.4.1 Полномочия на управление параметрами безопасности

Данные полномочия позволяют изменять параметры безопасности СЗИ ВИ.

Если пользователю (группе пользователей) разрешено изменение параметров безопасности, то он может делегировать все свои полномочия другим пользователям.

Для того чтобы назначить управление параметрами безопасности необходимо перейти на уровне Сервера УД во вкладку «Параметры безопасности домена» → «Права пользователей» (рис. 160).

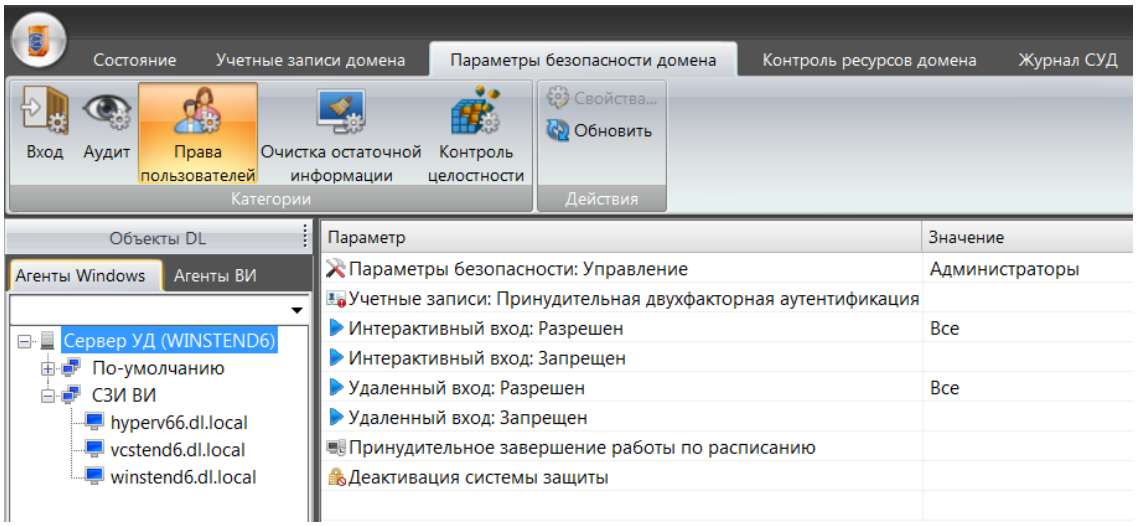


Рис. 160 – Управление правами пользователей

Выбрать в списке параметров «Параметры безопасности: Управление» и в категории «Действия» нажать кнопку «Свойства». Окно редактирования свойств параметра (рис. 161) также можно вызвать двойным кликом мыши на выбранном параметре либо из контекстно меню параметра, вызываемого нажатием правой кнопкой мыши.

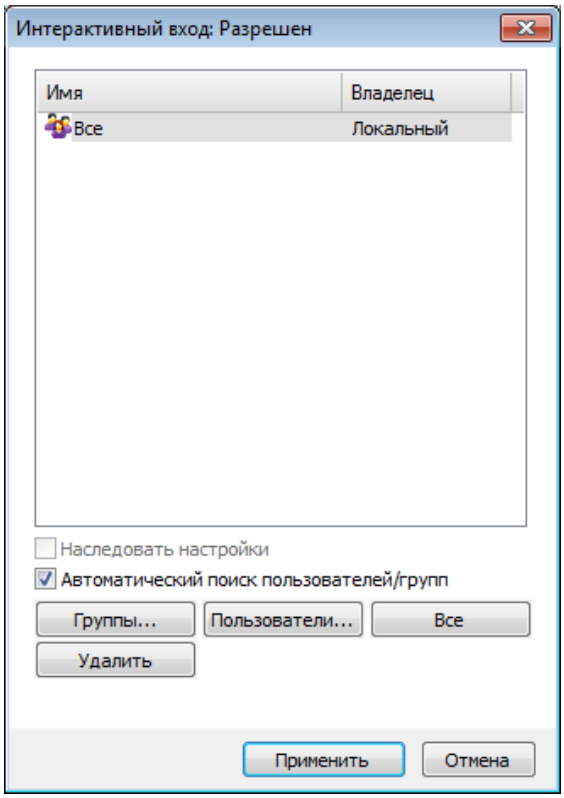


Рис. 161 – Добавление учетных записей

В список пользователей возможно добавлять, как отдельных пользователей, так и группы пользователей. Для добавления необходимо нажать на кнопку «Группы», либо «Пользователи». В появившемся окне необходимо выбрать размещение групп или пользователей (рис. 162), выбрать из списка необходимые и нажать кнопку «ОК».

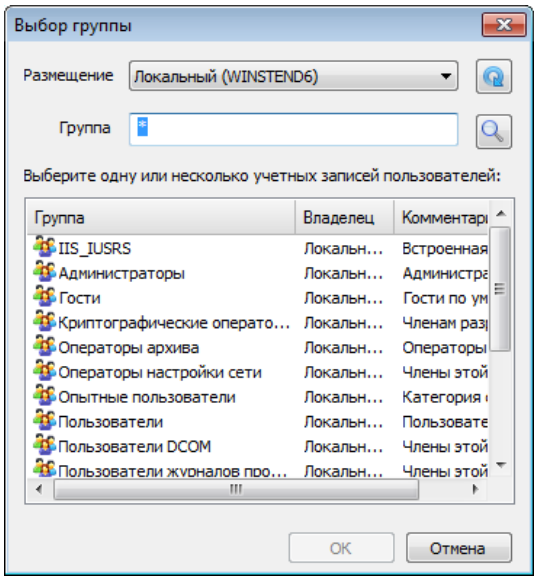


Рис. 162 – Выбор группы

Нажать кнопку «Применить».

Если пользователю предоставлено право на управление параметрами безопасности, то право на просмотр установленных настроек предоставляется автоматически.

5.4.2 Разрешение и запрет интерактивного и удаленного входов в ОС

СЗИ ВИ обеспечивает защиту информации от несанкционированного доступа на ПК в ЛВС через локальный и сетевой входы.

Выполнить настройку разрешения или запрета интерактивного, или удаленного входов в ОС данного ПК можно с помощью настройки параметров на уровне Сервера УД во вкладке «Параметры безопасности домена» → «Права пользователей» (рис. 160). С помощью параметров безопасности «Интерактивный вход: разрешен», «Интерактивный вход: запрещен», «Удаленный вход: разрешен» и «Удаленный вход: запрещен» определенным пользователям и группам можно запретить или разрешить локальный, или удаленный вход в ОС.

Чтобы добавить учетные записи в список разрешенных или запрещенных необходимо:

1. Выбрать параметр и в категории «Действия» нажать кнопку «Свойства» (рис. 161). Окно редактирования свойств параметра также можно вызвать двойным кликом мыши на выбранном параметре либо из контекстно меню параметра, вызываемого нажатием правой кнопкой мыши.
2. В список пользователей возможно добавлять, как отдельных пользователей, так и группы пользователей. Для добавления необходимо нажать на кнопку «Группы», либо «Пользователи». В появившемся окне необходимо выбрать размещение групп или пользователей, выбрать из списка необходимые и нажать кнопку «ОК».
3. Нажать кнопку «Применить».

При настройке следует учесть, что установленный параметр запрета имеет более высокий приоритет перед установленным параметром разрешения. Также следует обратить внимание на то, что удаленный ввод аппаратного идентификатора не поддерживается.

Правило разрешения и запрета действий следующее:

Условие	Результат
Нет никаких запретов и разрешений	Действие запрещено
Есть запись о разрешении, и нет записи о запрете	Действие разрешено
Есть запись о запрете	Действие запрещено, несмотря на наличие или отсутствие записи о разрешении

В списке субъектов, для которых устанавливается запрет или разрешение, определяется иерархия в порядке возрастания: группа «Все» → индивидуальная группа → учетная запись (доменная учетная запись «по маске») → пользователь.

Таким образом, чтобы субъекту (например, пользователю) действие было разрешено, то он не должен входить в состав субъекта (например, группы), для которого это действие имеет явный

запрет.

Пример:

Требуется настроить запрет входа в ОС для локальных пользователей (в доменной архитектуре).

Для запрета входа локальных пользователей необходимо изменить параметр «Интерактивный вход: разрешен» убрать учетную запись «Все» и добавить учетную запись «****». Если есть необходимость разрешения входа для пользователей определенного домена, то предварительно нужно создать учетную запись в виде «Имя_домена*» (см. п. 5.1.2.3 «Регистрация доменных учетных записей по маске»).

5.4.3 Настройка параметров безопасности

Для настройки политик безопасности необходимо перейти в дерево «Агенты Windows» и на уровне Сервера УД перейти во вкладку «Параметры безопасности домена». Настройки входа будут установлены для всех клиентов Windows в ДБ.

Настройки, касающиеся входа в систему, установки атрибутов пароля, аппаратных считывателей, регулируются в окне закладки «Вход» (рис. 163).

Примечание. Для того, чтобы при синхронизации на клиентах автоматически регистрировались считыватели аппаратных идентификаторов, необходимо их зарегистрировать на Сервере УД и отметить поле «Синхронизация настроек считывателей». Обязательным условием является предварительная установка драйверов идентификаторов на необходимых клиентах.

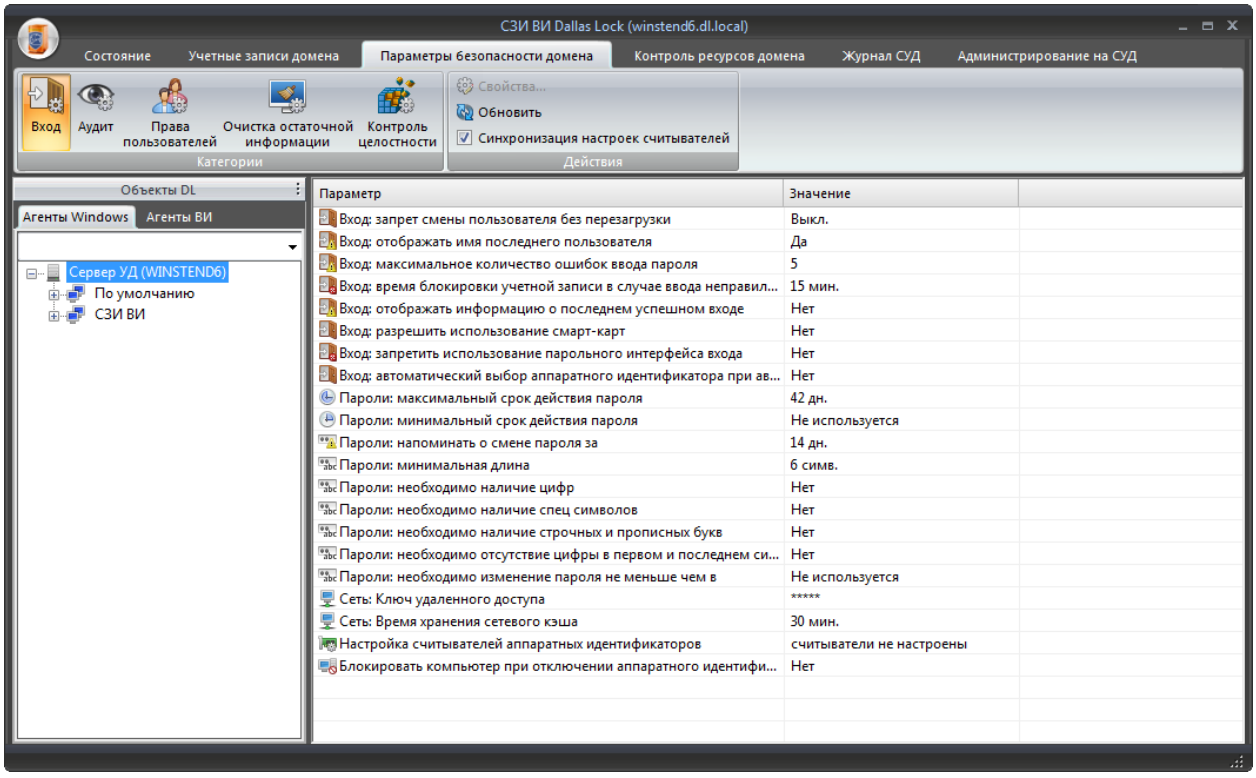


Рис. 163 – Параметры входа

В соответствии с требованиями политики безопасности организации необходимо настроить все параметры, расположенные в списке параметров на вход.

Вход: запрет смены пользователя без перезагрузки
Включение данного параметра не позволит осуществлять смену учетных записей пользователей без перезагрузки ПК. Если параметр имеет значение «Вкл.», то при выборе завершения сеанса или смены пользователя ПК автоматически уходит в перезагрузку. Данная политика позволяет предотвратить теоретическую возможность извлечения какой-либо информации из оперативной памяти ПК, оставшуюся там после завершения сеанса работы другого пользователя. По умолчанию параметр имеет значение «Выкл.», это означает, что при выборе завершения сеанса или смены пользователя ПК выйдет из учетной записи и предложит снова ввести авторизационные данные.

Вход: отображать имя последнего пользователя

Включение данного параметра позволяет отображать в окне авторизации имя учетной записи последнего пользователя, осуществлявшего вход в ОС.

По умолчанию параметр имеет значение «Да», это означает, что в поле, в котором требуется ввести имя пользователя при авторизации на ПК, будет отображаться имя последнего пользователя данного ПК. Если параметр имеет значение «Нет», то поле, в котором требуется ввести имя пользователя при авторизации на ПК, будет пустым.

Вход: максимальное количество ошибок ввода пароля

Значение, установленное для этого параметра, регламентирует, сколько раз пользователь имеет право ошибаться при вводе пароля. В выпадающем списке можно выбрать число попыток от 1 до 10.

Если при входе на защищенный компьютер или на этапе загрузки ОС пользователь ввел неверный пароль, то система выдаст предупреждение «Указан неверный пароль». Если число ошибок больше допустимого, учетная запись будет заблокирована, и пользователь не сможет загрузить компьютер и ОС. При этом система защиты выдаст сообщение «Запись пользователя заблокирована».

Способы разблокирования пользователей описаны в п.5.1.5 «Заблокированные пользователи».

Если установлено значение «Не используется», то пользователь может вводить неверный пароль неограниченное число раз.

По умолчанию значение данного параметра: 5.

Вход: время блокировки учетной записи в случае ввода неправильных паролей (мин.)

Данный параметр позволяет установить, сколько времени учетная запись будет заблокирована после того, как пользователь ввел неверный пароль больше допустимого числа раз. В этот временной интервал пользователь не сможет загрузить компьютер и ОС, даже при верном вводе пароля.

По истечении указанного времени учетная запись автоматически разблокируется, и пользователь снова получит возможность ввести пароль. Сбросить автоматическую блокировку досрочно может только администратор безопасности или пользователь, обладающий правом редактирования учетных записей.

Если при настройке опции выбрано значение «Не используется», то разблокировать учетную запись и тем самым позволить пользователю вновь работать на защищенном компьютере, может только администратор безопасности.

По умолчанию значение данного параметра: 15 мин.

Вход: отображать информацию о последнем успешном входе

При включении данного параметра входа (значение «Да») после загрузки ОС в области уведомлений Windows на панели задач будет появляться сообщение с информацией о дате последнего входа пользователя на данный компьютер, типе входа: сетевой, локальный, терминальный, неуспешных попытках входа и состоянии параметров учетной записи пользователя (рис. 164).

Рис. 164 – Всплывающее уведомление о последнем успешном входе

По умолчанию значение данного параметра: «Нет».

Вход: разрешить использование смарт-карт

Включение данного параметра разрешает использование микропроцессорных смарт-карт для авторизации в операционной системе Windows, при работе ПК в корпоративном домене. Смарт-карты применяются вместе с личными идентификационными номерами (PIN-кодами).

По умолчанию значение данного параметра: «Нет».

Вход: запретить использование парольного интерфейса входа

При использовании смарт-карт для авторизации в операционной системе возможно отключить интерфейс входа по имени пользователя и паролю, включением данного параметра.

По умолчанию значение данного параметра: «Нет».

Вход: автоматический выбор аппаратного идентификатора при авторизации

Включение данного параметра позволит автоматически выбрать подключенный аппаратный идентификатор при авторизации.

По умолчанию значение данного параметра: «Нет».

Пароли: максимальный срок действия пароля

Данным параметром устанавливается максимальный срок действия пароля для всех пользователей. По истечении установленного срока СЗИ ВИ автоматически предложит пользователю сменить пароль при входе в ОС. Если выбрано значение «Не используется», то время действия пароля не ограничено.

В тоже время, данный параметр не является приоритетным. Он действует, только если для пользователя не указано никаких иных значений срока действия пароля.

Максимальный срок действия пароля для каждого конкретного пользователя определяется по следующей схеме:

- Если администратор установил для конкретного пользователя принудительную смену пароля при следующем входе на компьютер, то в процессе очередной загрузки компьютера этим пользователем система защиты обязательно потребует сменить пароль, даже если срок действия пароля не истек (наивысший приоритет).
- Если администратором для конкретного пользователя *установлено* значение: Пароль без ограничения срока действия, и отсутствует требование смены пароля при следующем входе, то СЗИ ВИ не потребует смены пароля даже в случае превышения максимального срока действия пароля.
- Если администратором для конкретного пользователя *не установлено* значение: Пароль без ограничения срока действия, и отсутствует требование смены пароля при следующем входе, то СЗИ ВИ потребует от данного пользователя сменить пароль по истечении максимального срока действия пароля (низший приоритет).

По умолчанию значение данного параметра: 42 дн.

Пароли: минимальный срок действия пароля

Данным параметром устанавливается минимальный срок действия пароля для всех пользователей. До истечения установленного срока СЗИ ВИ не позволит пользователю сменить свой пароль. При выборе значения «Не используется» минимальный срок действия пароля не ограничен.

В тоже время, данный параметр не является приоритетным. Он действует, только если для пользователя не указано никаких иных значений срока действия пароля.

Минимальный срок действия пароля для каждого конкретного пользователя определяется по следующей схеме:

- Если администратор установил для конкретного пользователя принудительную смену пароля при следующем входе на компьютер, то в процессе очередной загрузки компьютера этим пользователем система защиты обязательно потребует сменить пароль (наивысший приоритет).
- Если отсутствует требование смены пароля при следующем входе, то СЗИ не позволит сменить пароль, если не истек установленный минимальный срок действия пароля. При этом на экране отобразится сообщение «Пароль не может быть изменен».
- Флажок в поле «Пароль без ограничения срока действия», установленный в настройках учетной записи, не даст возможности сменить пароль до окончания установленного минимального срока действия пароля.
- Если нарушено соотношение максимального и минимального сроков действия пароля (минимальный срок больше максимального), то СЗИ ВИ проигнорирует значение минимального срока действия пароля.

По умолчанию значение данного параметра: «Не используется».

Пароли: напоминать о смене пароля за (дн.)

С помощью данного параметра система защиты позволит напоминать пользователю о том, что через определенное количество дней необходимо сменить пароль. Если при настройке выбрать значение «Не используется», то напоминаний о необходимости смены пароля не будет.

Напоминание о предстоящей смене пароля будет появляться на экране при загрузке ОС данным пользователем, начиная с того момента, когда до смены пароля (фактически до истечения максимального времени действия пароля) осталось количество дней, равное установленному значению для этой политики.

По умолчанию значение данного параметра: 14 дн.

Примечание. Параметры, устанавливающие срок действия пароля, действуют независимо от аналогичных параметров ОС Windows. В Windows действуют свои политики безопасности, которые также могут потребовать смены пароля, независимо от СЗИ ВИ.

В СЗИ ВИ и ОС Windows совпадают следующие парольные политики:

- максимальный срок действия пароля;
- минимальная длина пароля;
- минимальный срок действия пароля;
- пароль должен отвечать требованиям сложности;

Чтобы не возникало конфликта парольных политик ОС Windows и Dallas Lock, нужно сделать данные политики идентичными в ОС и СЗИ, либо отключить политики в ОС.

Пароли: минимальная длина

Данным параметром устанавливается ограничение на минимальную длину пароля. Если число символов в пароле меньше установленного значения, то на экране появится предупреждение. При выборе значения «Не используется» устанавливаемый пароль может иметь пустое значение. Действие параметра распространяется на значения паролей, PIN-кодов и ключей.

При регистрации нового пользователя и при изменении старого пароля система защиты контролирует длину вводимого пароля. Если число символов в пароле меньше установленного значения, то на экране появится предупреждение «Ввод пароля: введен слишком короткий пароль».

Следует иметь в виду, что если в процессе работы изменено значение длину пароля (например, увеличена), то у зарегистрированных пользователей она останется прежней до первой смены ими пароля.

По умолчанию значение данного параметра: 6 симв.

Пароли: необходимо наличие цифр

Если данный параметр включен (значение «Да»), то при создании пароля в нем должны присутствовать цифры. Действие параметра распространяется на значения паролей, PIN-кодов и ключей.

Пример. У пользователя имеется пароль «password», если описанная выше опция активирована, то при смене пароля на «passwordd» выведется сообщение «В пароле должны содержаться цифры». Правильной будет смена пароля, например, с «password» на «password12».

По умолчанию значение данного параметра: «Нет».

Пароли: необходимо наличие спец. символов

Если данный параметр включен (значение «Да»), то при создании пароля в нем должны присутствовать специальные символы из следующего списка: ` ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; ‘ “ < > , . ? /.

Действие параметра распространяется на значения паролей, PIN-кодов и ключей.

Пример. Если у пользователя имеется пароль «password1», и если вышеописанная опция активирована, то при смене пароля на «password2» выведется сообщение «В пароле должны содержаться спецсимволы». Правильной будет смена пароля, например, с «password1» на «password#».

По умолчанию значение данного параметра: «Нет».

Пароли: необходимо наличие строчных и прописных букв

Если данный параметр включен (значение «Да»), то при создании пароля в нем должны присутствовать строчные и прописные буквы. Действие параметра распространяется на

значения паролей, PIN-кодов и ключей.

Пример: Если у пользователя имеется пароль «password1», и, если выше описанная опция активирована, то при смене пароля на «pacsword1» выведется сообщение «В пароле должны содержаться и строчные, и прописные буквы». Если пользователь сменит пароль «password1» на «paCsword1», то операция успешно завершится.

По умолчанию значение данного параметра: «Нет».

Пароли: необходимо отсутствие цифры в первом и последнем символе

Если данный параметр включен (значение «Да»), то при создании пароля на месте первого и последнего символа в нем не должны присутствовать цифры. Действие параметра распространяется на значения паролей, PIN-кодов и ключей.

По умолчанию значение данного параметра: «Нет».

Пароли: необходимо изменение пароля не меньше, чем в

Данным параметром задается количество символов, на которое, как минимум, должен отличаться новый пароль от старого, при его смене.

Если данный параметр включен, то при смене пароля через комбинацию клавиш «Ctrl + Alt + Del», новый пароль должен отличаться от старого не менее, чем на указанное количество символов. Сверка старого и нового пароля осуществляется посимвольно.

При смене пароля через Консоль данный параметр не учитывается.

Пример. У пользователя имеется пароль «password1», если в описанной выше опции количество символов указано 2, то при смене пароля «password1» на «password2» выведется сообщение «Пароль должен сильнее отличаться от предыдущего». Если пользователь сменит пароль «password1» на «Password2», то выведется сообщение «Пароль был успешно изменен» так как отличие старого пароля от нового составляет 2 символа.

Примечание. Следует учесть, что в ОС Windows есть свои, независимые политики сложности пароля. И в некоторых случаях пароль может удовлетворять политикам Dallas Lock, но не удовлетворять политикам Windows. В данном случае такой пароль установить не удастся.

По умолчанию значение данного параметра: «Не используется».

Сеть: Ключ удаленного доступа

Данным параметром устанавливается значение ключа удаленного доступа для удаленного входа на другие защищенные компьютеры. Подробнее – в п. 5.6 **«**Ключи удаленного доступа».

Сеть: Время хранения сетевого кэша

Для увеличения скорости работы по сети СЗИ ВИ предоставляет возможность сохранения сетевого кэша с информацией об имеющихся в сети компьютерах, которые защищены СЗИ ВИ, и к которым уже было произведено обращение с данного ПК. В выпадающем списке данного параметра можно выбрать время хранения такого сетевого кэша.

По умолчанию значение данного параметра: 30 мин.

Настройка считывателей аппаратных идентификаторов

С помощью данного параметра производится настройка считывателей электронных идентификаторов. Предварительно необходимо установить соответствующие драйверы и предъявить идентификаторы.

По умолчанию значение данного параметра: «Считыватели не настроены».

Блокировать компьютер при отключении аппаратного идентификатора

При включении данного параметра всем пользователям, которым назначен аппаратный идентификатор, работа на данном ПК при отключении идентификатора будет заблокирована. Параметр не распространяется на идентификаторы, предъявляемые по касанию.

По умолчанию значение данного параметра: «Нет».

5.4.4 Настройка средств аппаратной идентификации

СЗИ ВИ позволяет в качестве средства опознавания пользователей системы использовать аппаратные идентификаторы: USB-Flash накопители, электронные ключи Touch Memory (iButton), HID Proximity-карты, USB-ключи Aladdin eToken Pro/Java, смарт-карты Aladdin eToken PRO/SC, USB-ключи Рутокен (Rutoken), USB-ключи JaCarta и смарт-карты JaCarta, USB-ключи и смарт-карты ESMART Token, NFC-метки и смарт-карты семейства MIFARE.

При настройке аппаратного идентификатора рекомендуется устанавливать драйверы, поставляемые в комплекте с идентификатором, или скачать их с сайта производителя.

5.4.4.1 Общие сведения об идентификаторах

Электронный ключ Touch Memory представляет собой микросхему, размещенную в прочном корпусе из нержавеющей стали, по размерам и форме напоминающем батарейку от электронных часов (рис. 165).

Рис. 165 – Touch Memory

Фирма-производитель гарантирует, что у ключей Touch Memory не существует двух идентичных изделий (64-разрядный регистрационный номер). Аппаратная идентификация по Touch Memory возможна, только если установлена аппаратная часть. В качестве аппаратной части для работы с Touch Memory могут применяться:

- считыватель COM-A, подключаемый к COM-порту компьютера;
- считыватель COM-P, подключаемый к COM-порту компьютера.

Примечание. Идентификация по Touch Memory с помощью считывателей, подключаемых через COM-порт (COM-A, COM-P) возможна только при подключении через COM-порт, встроенный в системную плату или через кабель-преобразователь от USB на COM-порт.

Бесконтактная HID Proximity-карта представляет собой пластиковую карту со встроенной микросхемой и индивидуальным идентификационным кодом (рис. 166). Предназначена для контроля доступа и безопасной идентификации.

Примечание. Из-за особенностей работы драйверов считывателей HID (IronLogic) есть техническое ограничение на использование данного типа считывателей при авторизации через удаленный рабочий стол.

Рис. 166 – Бесконтактная HID Proximity-карта

Для использования подобных карт необходимо наличие специального считывателя (в СЗИ реализована поддержка считывателей HID IronLogic Z-2).

USB-ключ Aladdin eToken Pro/Java представляет собой защищенное устройство, предназначенное для строгой аутентификации и безопасного хранения секретных данных (рис. 167). USB-ключ eToken PRO/Java архитектурно реализован как USB-картридер с встроенной в него микросхемой (чипом) смарт-карты. Ключ выполнен в виде брелока и напрямую подключается к USB-порту компьютера, при этом не требует для своей работы каких-либо дополнительных устройств, кроме USB-порта.

Рис. 167 – Aladdin eToken Pro/Java

Смарт-карта Aladdin eToken PRO/SC представляет собой пластиковую карту со встроенной микросхемой (рис. 168). Она предназначена для строгой аутентификации, безопасного хранения секретных данных, выполнения криптографических вычислений и работы с асимметричными ключами и цифровыми сертификатами.

Рис. 168 – Смарт-карта Aladdin eToken PRO/SC

USB-ключи eToken Pro/Java и смарт-карты eToken Pro/SC имеют идентичную функциональность и выполнены на одной и той же микросхеме смарт-карты. Они одинаково поддерживаются использующими их приложениями.

Для корректной работы eToken (USB-ключей eToken Pro/Java и смарт-карт eToken Pro/SC) необходимо установить драйвера eToken PKI Client.

Электронный идентификатор Рутокен (Rutoken) – это компактное устройство в виде USB-брелока, которое служит для авторизации пользователя в сети или на локальном компьютере, защиты электронной переписки, безопасного удаленного доступа к информационным ресурсам, а также надежного хранения персональных данных. Рутокен представляет собой небольшое электронное устройство, USB-брелок, подключаемое к USB-порту компьютера (рис. 169).

Рис. 169 – Rutoken

СЗИ ВИ поддерживает работу с моделями Рутокен: Рутокен S, Рутокен Lite, Рутокен ЭЦП.

Электронные USB-ключи и смарт-карты JaCarta (JaCarta GOST и JaCarta PKI) представляют собой компактные устройства, предназначенные для обеспечения информационной безопасности корпоративных заказчиков и частных пользователей. Подобно персональному компьютеру устройства JaCarta содержат процессор и модули памяти, функционируют под управлением своей операционной системы, выполняют необходимые прикладные программы и хранят информацию. Микроконтроллеры для JaCarta проектируются для решения задач информационной безопасности: они обладают встроенной защищенной памятью, средствами противодействия атакам по питанию, криптографическим акселератором (рис. 170).

Рис. 170 – USB-ключ JaCarta

Смарт-карта ESMART Token (ESMART Token) представляет собой пластиковую карту со встроенной микросхемой (рис. 171). Смарт-карта обеспечивает безопасное хранение и использование цифровых сертификатов, ключей шифрования и электронной подписи. Для работы со смарт-картой ESMART Token требуется наличие считывателя контактных смарт-карт и свободный порт USB или RS-232 для подключения считывателя.

Рис. 171 – Смарт-карта ESMART Token

USB-ключ ESMART Token (ESMART Token) представляет собой защищенное устройство, предназначенное для строгой аутентификации и безопасного хранения секретных данных (рис. 172). USB-ключ ESMART Token представляет собой комбинацию считывателя и чипа смарт-карты в виде миниатюрного устройства. Устройство подключается к ПК напрямую, отдельный считыватель смарт-карт не требуется.

Рис. 172 – USB-ключ ESMART Token

NFC-метка и смарт-карта семейства MIFARE представляют собой брелок (наклейку) и пластиковую карту со встроенным чипом NFC соответственно. Для работы требуется наличие считывателя бесконтактных смарт-карт.

На диске с дистрибутивом системы защиты имеются необходимые драйверы для настройки аппаратной идентификации при работе с различными ОС.

Таблица 1. Список директорий с драйверами на диске с дистрибутивом

Название папки с дистрибутивом		Назначение
Aladdin	Athena для eToken SmartCard	Дистрибутив для установки считывателя смарт-карт eToken от поставщика компании «Аладдин»
	PKI Client	Дистрибутив для установки драйверов традиционного USB-ключа eToken PKI Client от поставщика компании «Аладдин»
ATEN UC-232A USB-COM		Дистрибутив для установки драйверов кабеля-преобразователя от USB на COM-порт Aten UC-232A (для считывателей Touch Memory, подключаемых к COM-порту)
Rutoken		Драйверы идентификаторов Рутокен
USB to Serial RDS		Дистрибутив для установки драйвера считывателя Touch Memory Aladdin RDS-02 USB
JaCarta		Дистрибутивы для установки драйверов идентификаторов JaCarta
HID		Дистрибутив для установки драйвера считывателя HID IronLogic Z-2
ESMART Token		Дистрибутив для установки драйвера идентификаторов ESMART Token
NFC		Дистрибутив для установки драйвера идентификаторов NFC

Примечание. Кабель-преобразователь ATEN UC-232A поддерживает все ОС, с которыми работает СЗИ ВИ, кроме Windows Server 2008. Если есть необходимость, то существуют другие преобразователи с заявленной поддержкой данной операционной системы, например, конверторы фирм-производителей Valley Enterprises, Digi, MANHATTAN, «Лаборатория электроники».

5.4.4.2 Настройка считывателей аппаратных идентификаторов

Перед настройкой идентификации с помощью аппаратных средств необходимо установить соответствующие драйверы. Установка драйверов возможна как перед установкой на ПК СЗИ ВИ, так и после.

Для дальнейшей работы необходима регистрация или настройка считывателей в СЗИ ВИ.

1. После того, как считыватель аппаратного идентификатора и драйверы к нему установлены, необходимо войти в Консоль, в дереве «Агенты Windows» на уровне Сервера УД открыть «Параметры безопасности домена» → «Вход» → «Настройка считывателей аппаратных идентификаторов». На экране отобразится окно настройки (рис. 173).

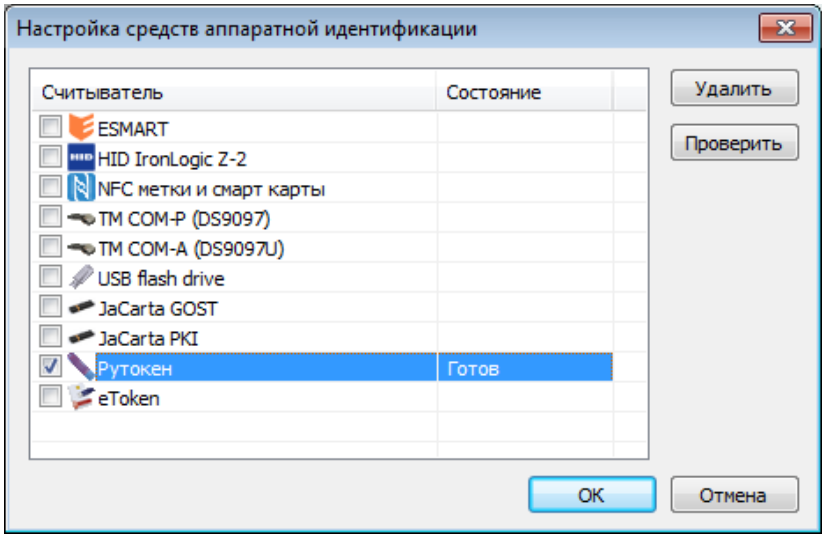


Рис. 173 – Окно настройки средств аппаратной идентификации

Окно имеет поля по настройке считывателей идентификаторов Touch Memory, USB-Flash-накопитель, USB-ключи JaCarta, Рутокен, Aladdin eToken, ESMART Token, NFC метки и смарт-карты семейства MIFARE.

2. Выделив необходимый идентификатор нужно нажать «Добавить» или поставить флаг. Кнопка «Проверить» станет активной.
3. Перед проверкой готовности идентификатора необходимо его предъявить или настроить:
   - **3.1.** Для настройки аппаратных идентификаторов типа Touch Memory и HID необходимо подключить аппаратный считыватель к компьютеру через COM–порт (или USB для HID считывателя) и определить с помощью Диспетчера устройств Windows номер соответствующего COM–порта (рис. 174).

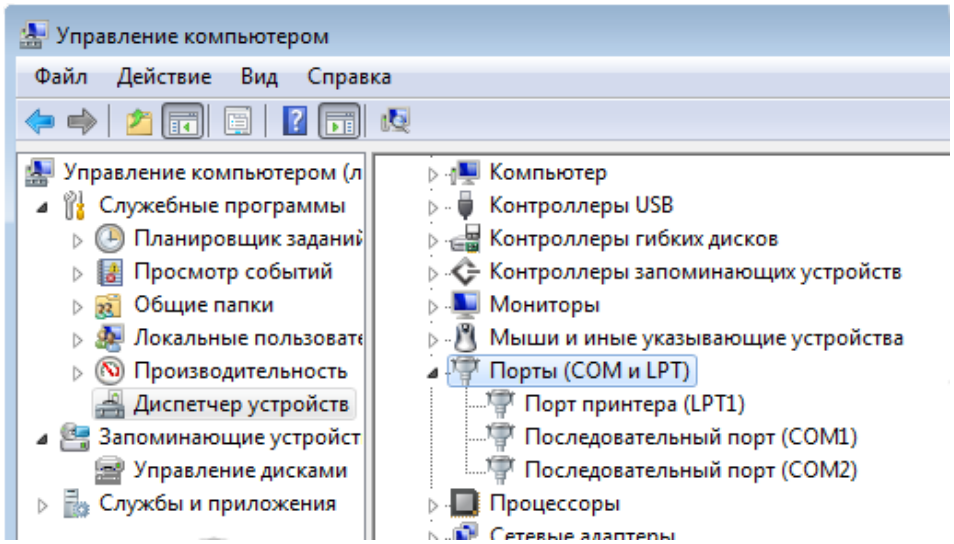


Рис. 174 – Окно Диспетчера устройств Windows

В окне настройки средств аппаратной идентификации нужно выбрать название аппаратного идентификатора в списке и нажать кнопку «Добавить». На экране появится окно для выбора, соответствующего COM–порта для подключенного идентификатора (рис. 175).

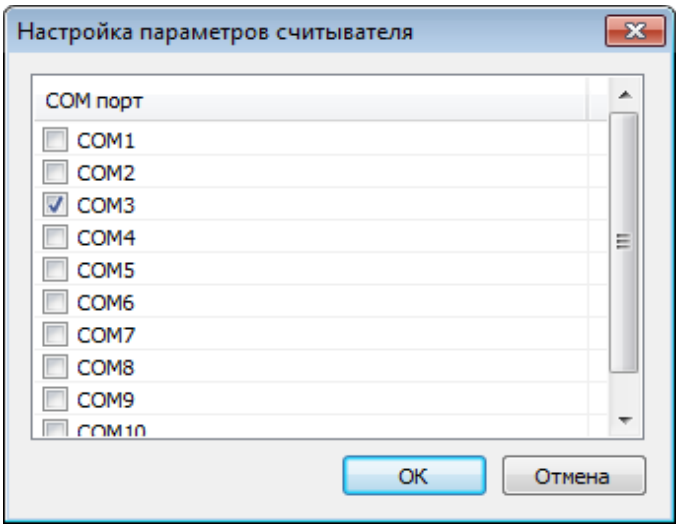


Рис. 175 – Выбор com-порта подключенного считывателя идентификатора

В окне со списком COM-портов нужно установить соответствующий флаг и нажать «ОК».

3.2. Для настройки аппаратного идентификатора типа смарт-карта eToken Pro/SC к соответствующему порту необходимо подключить считыватель смарт-карты.

Для идентификатора типа смарт-карта eToken Pro/SC флаг необходимо поставить в поле «eToken».

3.3. Для идентификатора типа USB-ключ JaCarta флаг необходимо поставить в соответствующее идентификатору поле.

3.4. Для идентификатора типа Рутокен флаг необходимо поставить в поле «Рутокен».

3.5. Для настройки аппаратного идентификатора типа смарт-карта ESMART Token к соответствующему порту необходимо подключить считыватель смарт-карты.

Для идентификатора типа смарт-карта ESMART Token флаг необходимо поставить в поле «ESMART».

Для идентификатора типа USB-ключ ESMART Token флаг необходимо поставить в поле «ESMART».

3.6. Для идентификатора типа NFC метки флаг необходимо поставить в поле «NFC метки и смарты карты».

4. После этого необходимо проверить состояние идентификатора, нажав соответствующую кнопку «Проверить» и прикоснувшись идентификатором к считывателю, или (в случае настройки USB-Flash накопителя, eToken, Рутокен, USB-ключа JaCarta, USB-ключа ESMART Token) подключить USB-устройство идентификатора к компьютеру.

В случае успешного подключения в строке состояния появится сообщение **«Готов»**.

После настройки подключенных к системе аппаратных идентификаторов их можно назначать в качестве средств идентификации для входа пользователя в настройках учетной записи и для преобразования информации.

Удалить настройки считывателя идентификатора можно, выбрав его из списка и нажав появившуюся кнопку «Удалить».

Примечание. Следует обратить внимание, что аппаратный идентификатор типа eToken NG-FLASH определяется в системе как USB-flash-drive.

Примечание. Для тестирования правильности подключения считывателей Touch Memory и автоматического определения типа считывателя и номера COM порта рекомендуется использовать программу iButton Viewer version 3.20 от фирмы Dallas Semiconductors.

Следует обратить внимание, что политика безопасности «Настройка считывателей аппаратных идентификаторов» нужна для указания типа подключенных аппаратных идентификаторов в системе. На проверку идентификационной информации пользователя она не влияет. Поэтому, если, например, настроить считыватель, задать пользователю аппаратный идентификатор, а после очистить настройки аппаратных считывателей, то при входе данного пользователя аппаратный

идентификатор будет проверяться все равно, и, соответственно, он не сможет войти в систему. Если задан пользователю аппаратный идентификатор – система защиты обязана его проверить, а если проверить нельзя, то допустить пользователя до информационных ресурсов система защиты не имеет права.

Примечание. Если пользователю присвоен аппаратный идентификатор, то функция операционной системы «Запуск от имени…» этому пользователю будет не доступна.

Примечание. При возникновении ошибок в процессе аутентификации и разблокировки ПК по аппаратным идентификаторам eToken PRO (32/64K) (смарт-карта) и eToken PRO (Java 72K) (смарт-карта) необходимо следующее:

1. Для разблокирования и аутентификации требуется отключить и снова подключить считыватель смарт-карты.
2. Для устранения самой ошибки следует выполнить действия:
   - **2.1.** Зайти в диспетчер устройств.
   - **2.2.** Найти «Устройство чтения смарт-карт».
   - **2.3.** Открыть «Управление электропитанием».
   - **2.4.** Снять флаг с «Разрешить отключение этого устройства для экономии энергии».

5.5 Аппаратная идентификация пользователя

Практически все решения защиты информационных ресурсов основаны на доступе, с использованием персональных паролей.

Дополнительное использование аппаратной идентификации позволяет решить проблему человеческого фактора, связанного с хранением сложных паролей, и усилить защиту информации.

5.5.1 Назначение аппаратной идентификации

Перед назначением аппаратного идентификатора следует:

1. Установить драйвер соответствующего идентификатора.
2. Настроить в системе защиты его считыватель.

Подробное описание настройки считывателей приведено в п. 5.4.4 «Настройка средств аппаратной идентификации» данного руководства.

Для назначения идентификатора пользователю, необходимо в дереве «Агенты Windows» на уровне Сервера УД перейти на вкладку «Учетные записи домена» → «Учетные записи», открыть окно создания или редактирования учетной записи пользователя и перейти на закладку «Аппаратная идентификация» (рис. 176).

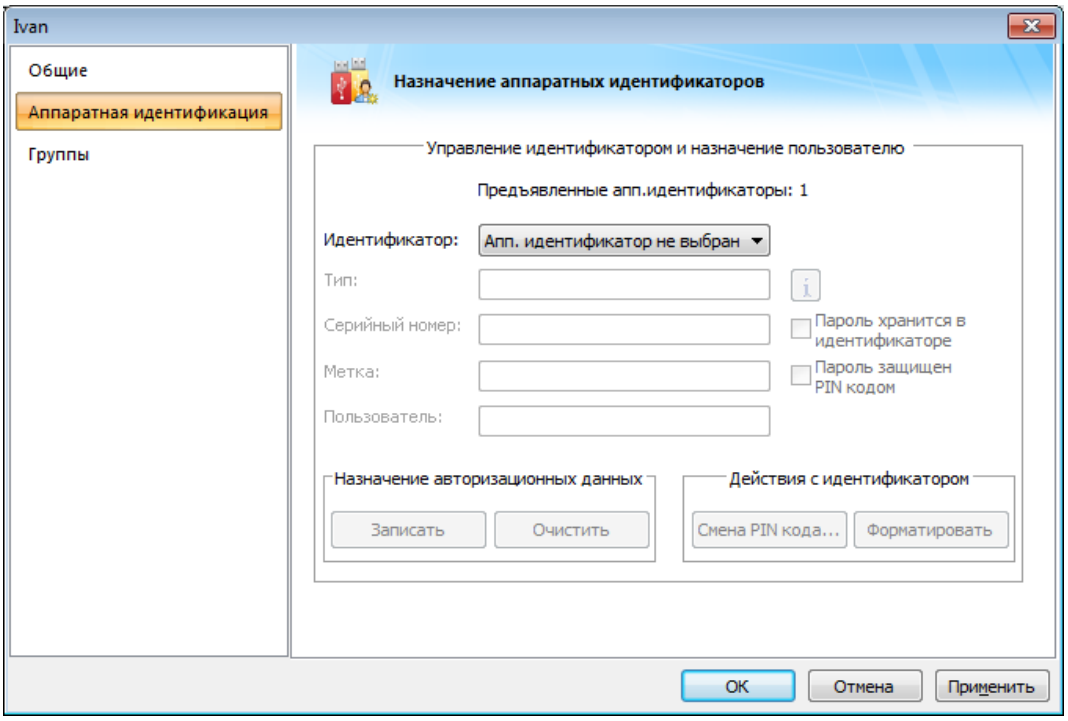


Рис. 176 – Вкладка назначения аппаратных идентификаторов пользователю

Необходимо предъявить аппаратный идентификатор. Предъявить идентификатор можно, в зависимости от типа, вставив его в соответствующий USB-порт, или прикоснувшись к считывателю. В строке состояния «Предъявленные аппаратные идентификаторы» появится цифра с количеством идентификаторов, предъявленных в данный момент, а в списке выпадающего меню – наименования. Следует выбрать необходимый идентификатор из списка.

После выбора идентификатора в полях с параметрами появятся: наименование его типа, номер, изображение и, для некоторых видов идентификаторов[22], станут доступны дополнительные функции (рис. 177).

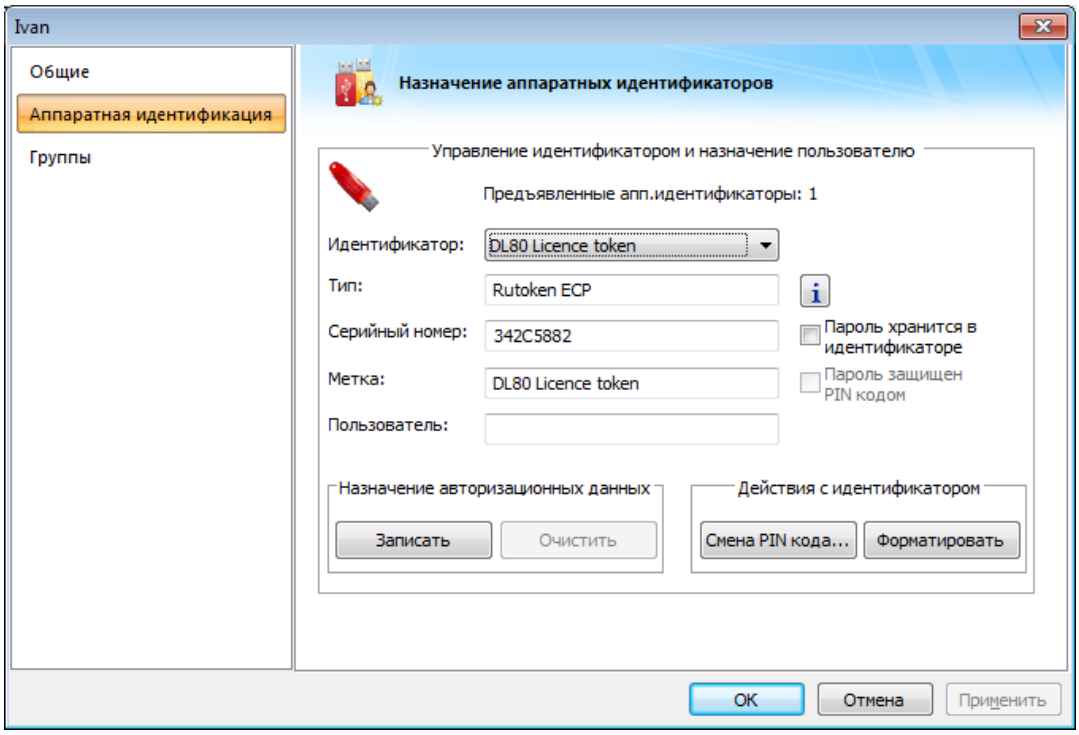


Рис. 177 – Параметры назначенного идентификатора

После выбора идентификатора для пользователя необходимо нажать «Применить» и «OK». Таким образом, после назначения идентификатора для учетной записи, для входа в ОС помимо ввода

[22] USB-ключи Aladdin eToken Pro/Java, смарт-карты Aladdin eToken PRO/SC, USB-ключи Рутокен (Rutoken), USB-ключи и смарт-карты JaCarta, USB-ключи и смарт-карты ESMART Token.

авторизационной информации, станет необходимо предъявить и назначенный аппаратный идентификатор.

После выбора предъявленного идентификатора дополнительная кнопка позволяет открыть окно с информацией о параметрах данного идентификатора.

5.5.2 Принудительная двухфакторная аутентификация

В СЗИ ВИ для учетной записи пользователя или группы пользователей может быть установлена обязательная двухфакторная аутентификация для входа в ОС: аутентификация с вводом пароля и предъявлением назначенного аппаратного идентификатора.

Функционально для обязательной двухфакторной аутентификации необходимо выполнение двух условий:

1. Для параметра сложности паролей «Пароли: минимальная длина» не должно быть установление значение «Не используется».
2. Для параметра безопасности «Учетные записи: Принудительная двухфакторная аутентификация» в значении должны быть выбраны необходимые учетные записи пользователей или группы.

За последнее отвечает параметр «Учетные записи: Принудительная двухфакторная аутентификация» (в дереве «Агенты Windows» на уровне Сервера УД во вкладке «Параметры безопасности домена» → «Права пользователей»). Если в значении данного параметра стоит определенная учетная запись или группа, то при регистрации новой учетной записи (в составе данной группы или индивидуально) присвоение идентификатора будет обязательным, иначе будет выведено предупреждение об ошибке.

5.5.3 Снятие аппаратной идентификации

Для того чтобы снять назначение аппаратного идентификатора для учетной записи отдельного пользователя, необходимо на закладке «Аппаратная идентификация» окна параметров учетной записи в меню отображения имени идентификатора выбрать значение «Аппаратный идентификатор не назначен» нажать «Применить» и «ОК».

Сам идентификатор для последующего применения рекомендуется очистить от авторизационных данных, если они были назначены (см. ниже) или отформатировать.

5.5.4 Дополнительные возможности аппаратной идентификации

5.5.4.1 Действия с идентификатором

Для идентификаторов типа USB-ключи Aladdin eToken Pro/Java, смарт-карты Aladdin eToken PRO/SC, USB-ключи Рутокен (Rutoken), USB-ключи и смарт-карты JaCarta (JaCarta GOST и JaCarta PKI), USB-ключи и смарт-карты ESMART Token (ESMART Token ГОСТ) доступны дополнительные расширенные возможности аппаратной идентификации.

Для работы с данными аппаратными идентификаторами необходимы их авторизационные PIN-коды: PIN-код администратора и PIN-код пользователя, которые уже установлены в памяти самих идентификаторов по умолчанию (так называемые «заводские настройки»). Информацию о них можно получить из документации, поставляемой вместе с аппаратными идентификаторами и драйверами.

Для обеспечения требуемого уровня безопасности данные PIN-коды следует изменить. Это можно также сделать, воспользовавшись специальной утилитой для идентификатора, либо используя окно параметров назначенного пользователю идентификатора в оболочке администратора системы защиты. Для этого в поле «Действия с идентификатором» необходимо выбрать кнопку «Смена PIN-кода» или кнопку «Форматировать».

По нажатию кнопки «Смена PIN-кода» откроется окно, в котором необходимо ввести значения PIN-кода пользователя: старое (текущее) значение, новое значение и повтор. Дополнительные кнопки рядом с полями ввода позволят изменить скрытые под звездочками символы на явные, повтор ввода PIN-кода в этом случае не потребуется (рис. 178).

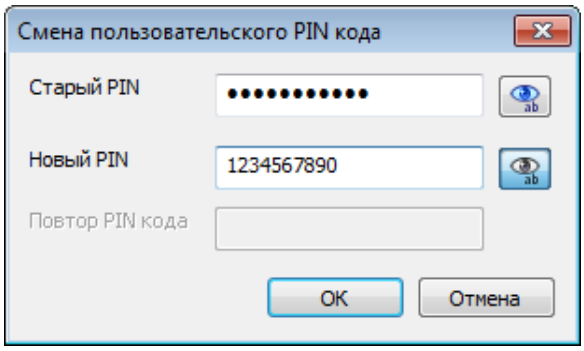


Рис. 178 – Окно смены PIN-кода

По нажатию кнопки «Форматировать» откроется окно форматирования аппаратного идентификатора (рис. 179), в котором необходимо заполнить следующие поля:

- **Текущий PIN-код администратора** данного аппаратного идентификатора, необходимый для легального форматирования идентификатора.

Ввести новые данные:

- **Метка** – любое наименование;
- **Новый PIN-код** администратора и повтор;
- **Новый PIN-код** пользователя и повтор.

Если два данных PIN кода должны совпасть, то флаг в поле «PIN-код администратора и пользователя совпадают» позволит ввести PIN-код только в одно поле.

Внимание. Параметры символов PIN-кода для идентификатора (наличие цифр, букв и другие) определяются настройкой параметров в утилите соответствующего идентификатора. И, прежде чем изменять PIN-коды идентификатора, следует настроить данные параметры именно в утилите, которые по умолчанию **выключены.**

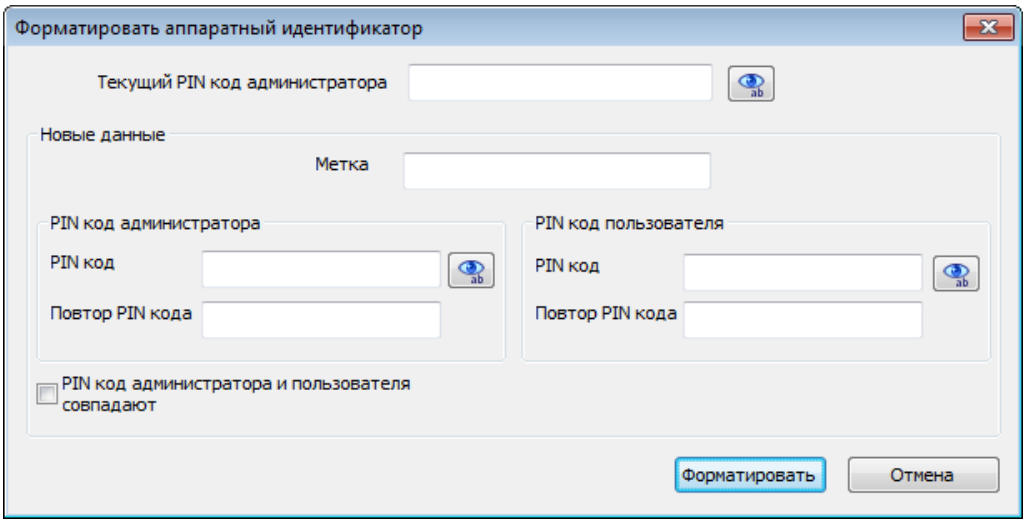


Рис. 179 – Окно форматирования идентификатора

5.5.4.2 Запись авторизационных данных в идентификатор

Запись авторизационных данных в память идентификатора доступна для следующих типов: USB-ключи Aladdin eToken Pro/Java, смарт-карты Aladdin eToken PRO/SC, USB-ключи Рутокен (Rutoken), USB-ключи и смарт-карты JaCarta, USB-ключи и смарт-карты ESMART Token.

Записать в память аппаратного идентификатора авторизационные данные (логин и пароль) учетной записи пользователя, которому он назначается, можно тремя способами:

1. Записать в память идентификатора логин и пароль пользователя и хранение данных защитить PIN-кодом. Для этого необходимо выполнить следующее. После выбора в выпадающем списке необходимого идентификатора, отметить флажком поле «Пароль хранится в идентификаторе». Поле «Пароль защищен PIN-кодом» выделится автоматически. Затем нажать кнопку «Записать» (рис. 180).

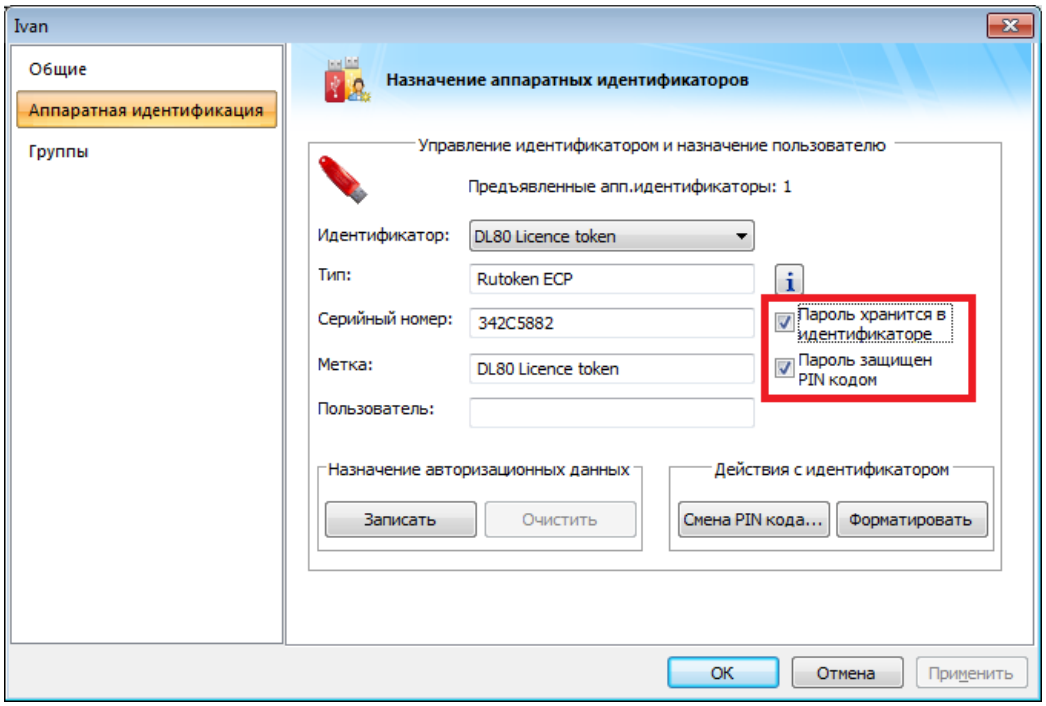


Рис. 180 – Запись авторизационной информации в идентификатор

Далее, в появившемся окне ввести дополнительную информацию (PIN-код пользователя идентификатора и пароль пользователя) и нажать «OK» (рис. 181).

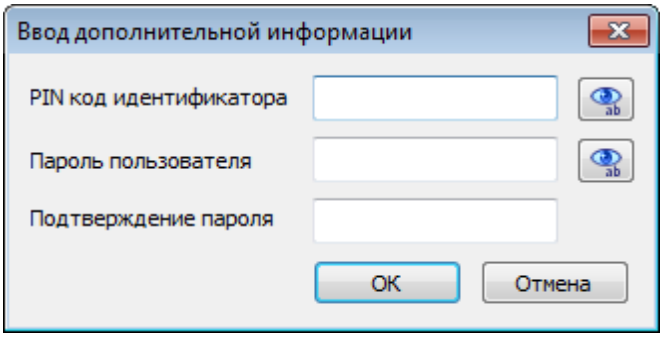


Рис. 181 – Ввод дополнительной информации

В окне параметров учетной записи системы защиты нажать «Применить» и «OK».

После этого в память данного идентификатора будет прописан логин и пароль учетной записи пользователя, причем пароль будет защищен PIN-кодом самого идентификатора.

Теперь для входа в ОС после предъявления идентификатора пользователю необходимо заполнить только поле ввода PIN-кода (логин и пароль считаются автоматически, для считывания пароля потребуется ввод PIN-кода).

2. Записать в память идентификатора логин и пароль учетной записи. Для этого необходимо выполнить следующее. В поле «Пароль защищен PIN-кодом» снять флаг, и таким образом записать авторизационные данные (кнопка «Записать»). Но в этом случае пароль учетной записи в идентификаторе будет незащищен, и система выдаст предупреждение. Таким образом, для входа в ОС пользователю станет достаточным только предъявление идентификатора (логин и пароль считаются автоматически).
3. Записать в память идентификатора только логин учетной записи пользователя. Для этого не требуется выделение полей хранения паролей. Достаточно нажатия кнопки «Записать». Система потребует ввести дополнительно только PIN-код пользователя данного идентификатора. При входе в ОС после предъявления идентификатора учетная запись будет однозначно идентифицирована с логином данного конкретного пользователя, остальные авторизационные поля пользователю необходимо будет ввести самостоятельно.

Для того чтобы стереть авторизационную информацию из памяти идентификатора, нужно воспользоваться одним из следующих способов:

- Воспользоваться кнопкой «Очистить» в поле назначения авторизационных данных.
- Отформатировать идентификатор методом, описанным выше. В этом случае помимо удаления системой защиты авторизационных данных из памяти идентификатора администратору безопасности необходимо изменить PIN-коды идентификатора.

Авторизация с записанными данными возможна при входе в ОС после включения компьютера, а также при входе при разблокировке и терминальном подключении.

Вход в операционную систему защищенного компьютера с использованием аппаратного идентификатора подробно описан в разделе «Вход с аппаратным идентификатором».

5.5.4.3 Определение принадлежности идентификатора

В СЗИ ВИ реализован механизм, с помощью которого, предъявив аппаратный идентификатор, можно определить, какому пользователю он принадлежит.

Чтобы открыть окно с информацией об идентификаторе, необходимо сначала его предъявить (приложить к считывателю или вставить в USB-порт). Далее в Консоли в дереве «Агенты Windows» перейти на вкладку «Учетные записи» и нажать кнопку «Принадл. идентификатора» (рис. 182).

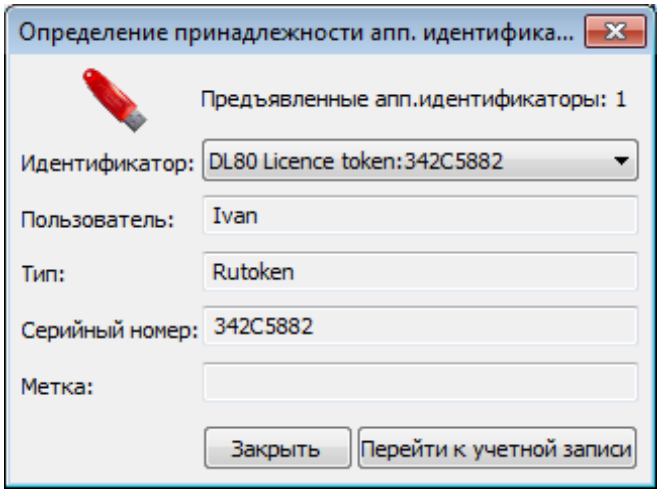


Рис. 182 – Окно свойств предъявленного идентификатора

В появившемся окне после выбора из выпадающего списка идентификатора появится информация о его типе и владельце. Если владелец определен, то из данного окна можно перейти к просмотру и редактированию учетной записи пользователя, которому идентификатор назначен.

5.5.5 Вход с использованием смарт-карт с сертификатом УЦ Windows

Для возможности входа на компьютер с установленным на нем СЗИ ВИ Dallas Lock при помощи смарт-карт, через удостоверяющий центр MS Windows, необходимо соблюдение следующих условий:

- компьютер, на который осуществляется вход, должен быть введен в доменную сеть Windows и находиться под управлением Active Directory;
- в Консоли ЦУ СЗИ ВИ Dallas Lock в дереве «Агенты Windows» во вкладке «Параметры безопасности домена» в категории «Вход» включена политика СЗИ ВИ «Вход: разрешить использование смарт-карт» (подробнее см. п. 5.4.3 «Настройка параметров »).

Если все условия соблюдены, экран приветствия будет содержать отдельную опцию, позволяющую войти в ОС с использованием смарт-карт (рис. 183, рис. 184)

Рис. 183 – Экран приветствия в ОС Windows 7

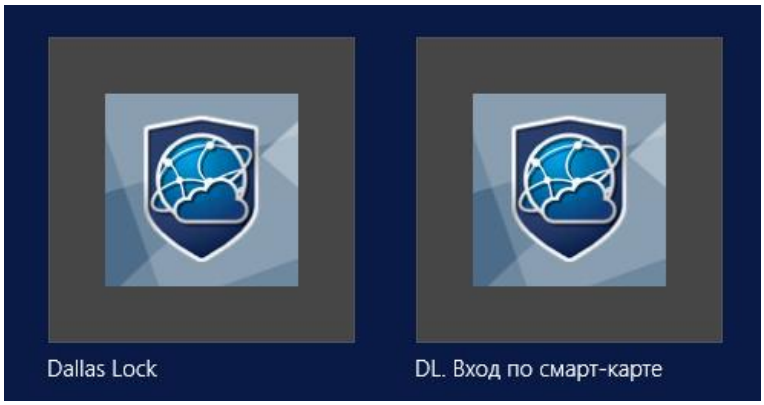


Рис. 184 – Экран приветствия в ОС Windows Server 2012 R2

При выборе входа по смарт карте необходимо вставить смарт карту в считывающее устройство, ввести PIN-код и нажать кнопку «Enter» (рис. 185).

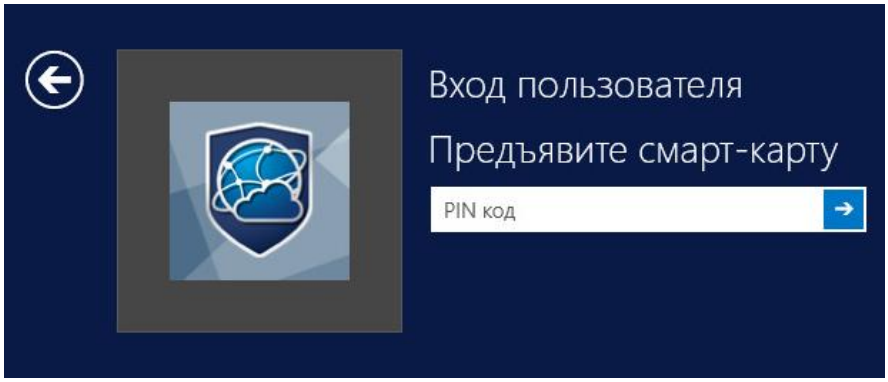


Рис. 185 – Экран входа по смарт-карте в ОС Windows Server 2012 R2

5.5.6 Вход с аппаратным идентификатором

Если пользователю в процессе работы назначен аппаратный идентификатор, то, для того чтобы его предъявить, необходимо выполнить следующие шаги:

1. В зависимости от типа устройства предъявить идентификатор можно, вставив его в USB-порт, или прикоснувшись к считывателю.
2. Необходимо выбрать наименование идентификатора из списка, который появится в выпадающем меню в поле «Аппаратные идентификаторы» (рис. 186).

Рис. 186 – Выбор аппаратного идентификатора при входе в ОС Windows

При подключении единственного идентификатора он будет выбран автоматически.

3. Далее, в зависимости от настроек, произведенных администратором безопасности применительно к учетной записи пользователя, возможны следующие способы авторизации:
   - **3.1.** Выбор аппаратного идентификатора и заполнение всех авторизационных полей формы (рис. 187).

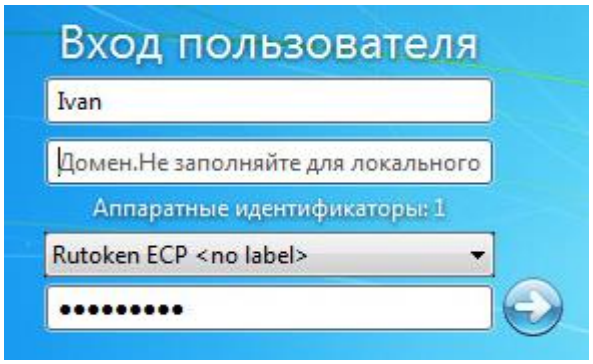


Рис. 187 – Поля авторизации после предъявления идентификатора

3.2. Выбор аппаратного идентификатора и ввод только пароля (логин автоматически считывается с идентификатора) (рис. 188):

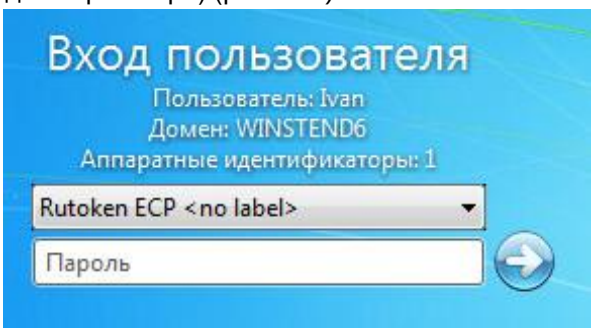


Рис. 188 – Поля авторизации после предъявления идентификатора

3.3. Выбор только аппаратного идентификатора (логин и пароль автоматически считываются с идентификатора) (рис. 189):

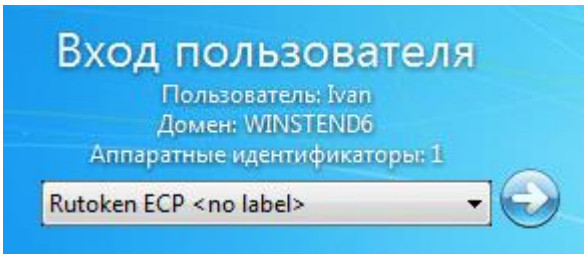


Рис. 189 – Поля авторизации после предъявления идентификатора

3.4. Выбор аппаратного идентификатора и ввод только PIN-кода идентификатора (логин и пароль автоматически считываются с идентификатора) (рис. 190):

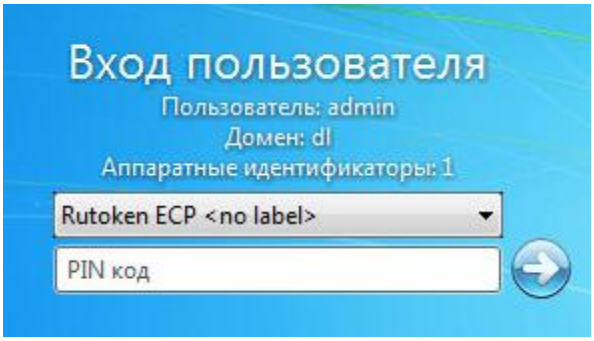


Рис. 190 – Поля авторизации после предъявления идентификатора

5.6 Ключи удаленного доступа

Каждый защищенный системой СЗИ ВИ компьютер имеет ключ удаленного доступа. Пользователи могут осуществлять удаленный вход на защищенные компьютеры (при условии соблюдения остальных условий) только при совпадении ключей удаленного доступа.

На всех защищенных компьютерах в ЛВС, после установки СЗИ ВИ с файлом конфигурации по умолчанию, зарегистрирован ключ удаленного доступа с пустым значением. Однако в системе реализована возможность изменения ключа удаленного доступа на компьютере. Для этого в Консоли на вкладке «Параметры безопасности домена» в категории политик безопасности «Вход» необходимо выбрать из списка и открыть параметр «Сеть: Ключ удаленного доступа» и заполнить

требуемые поля (рис. 191).

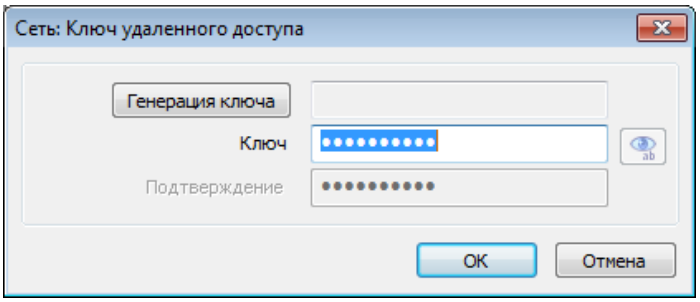


Рис. 191 – Окно ввода нового ключа удаленного доступа

Рекомендуется вводить и изменять настройки ключей удаленного доступа только опытным специалистам, и только в тех случаях, когда это действительно необходимо. Так как неосторожная смена ключа доступа у одного ПК, может привести к тому, что удаленный доступ на него будет невозможен.

Для создания ключа удаленного доступа, отвечающего всем требованиям параметров безопасности, установленных СЗИ ВИ, можно воспользоваться помощью генератора паролей. Для этого следует нажать поле с надписью «Генерация ключа». Система автоматически создаст уникальный ключ, значение которого необходимо ввести в поля «Ключ» и «Подтверждение».

Дополнительная кнопка  изменит скрытые символы на явные. Подтверждение в этом случае не потребуется и заблокируется.

Примечание. Политики сложности паролей распространяются и на установку значений для ключа удаленного доступа. Поэтому, чтобы была возможность задать пустое значение ключа удаленного доступа, необходимо, чтобы параметр «Пароли: минимальная длина» имел значение «Не используется».

6 ПОДСИСТЕМА УПРАВЛЕНИЯ ДОСТУПОМ

6.1 Разграничение доступа к объектам ФС ОС Windows

Одной из главных задач любой системы защиты информации от несанкционированного доступа является разграничение доступа. В СЗИ ВИ реализована настройка разграничения доступа к объектам файловой системы и к подключаемым устройствам. СЗИ ВИ позволяет гибко и удобно задавать пользователям права на доступ. После задания прав пользователи могут работать только с теми объектами, доступ к которым им разрешен, и совершать над ними только санкционированные операции.

В СЗИ ВИ предусмотрен принцип разграничения прав согласно индивидуальному списку доступа к объекту – дискреционный доступ.

СЗИ ВИ позволяет разграничивать доступ ко всем объектам ФС (кроме объектов vCSA и ESXi): файлам, папкам, дискам, которые могут располагаться как на локальных дисках клиентов, так и на сменных и сетевых. Подробное описание разграничения доступа к объектам ФС приводится ниже.

СЗИ ВИ позволяет разграничивать доступ к подключаемым устройствам. Подробнее о разграничении доступа к устройствам в п. 6.2 «Контроль устройств в ОС Windows».

6.1.1 Дескрипторы объектов

Дескриптор — это символический идентификатор назначенного для объекта файловой системы (или устройства) правила доступа.

Глобальные параметры доступа к объектам ФС называют **«глобальными дескрипторами»**, тогда как совокупность всех параметров безопасности (дискреционный доступ, аудит, контроль целостности), назначенных на какой-либо объект файловой системы, называют **дескриптором** этого объекта.

Соответственно, операция назначения каких-либо параметров безопасности на объект файловой системы (или устройства) называется «**создать дескриптор**», «**назначить дескриптор**» или даже «**повесить дескриптор**».

Дескрипторы объектов в свою очередь делятся на **дескрипторы дискреционного доступа**, **дескрипторы аудита**, **дескрипторы контроля целостности**. Дескриптор дискреционного доступа, это дескриптор, содержащий только параметры дискреционного доступа, дескриптор аудита, это дескриптор, содержащий только параметры аудита и т.д.

Точно также дескрипторы делятся на **локальные дескрипторы** (назначенные локальным объектам ФС или конкретным устройствам), **сетевые дескрипторы** (назначенные объектам ФС, расположенным в сети), **сменные дескрипторы** (назначенные объектам, расположенным на сменных накопителях). Дескрипторы бывают **дескрипторами файлов** (назначенные на файл), **дескрипторами папок** (назначенные на папку), **дескрипторами устройства**, например, **дисков** (назначенные на диск).

В дальнейшем, в контексте данного руководства, под понятием «дескриптор» будет пониматься также и окно с параметрами доступа выбранного объекта (рис. 192).

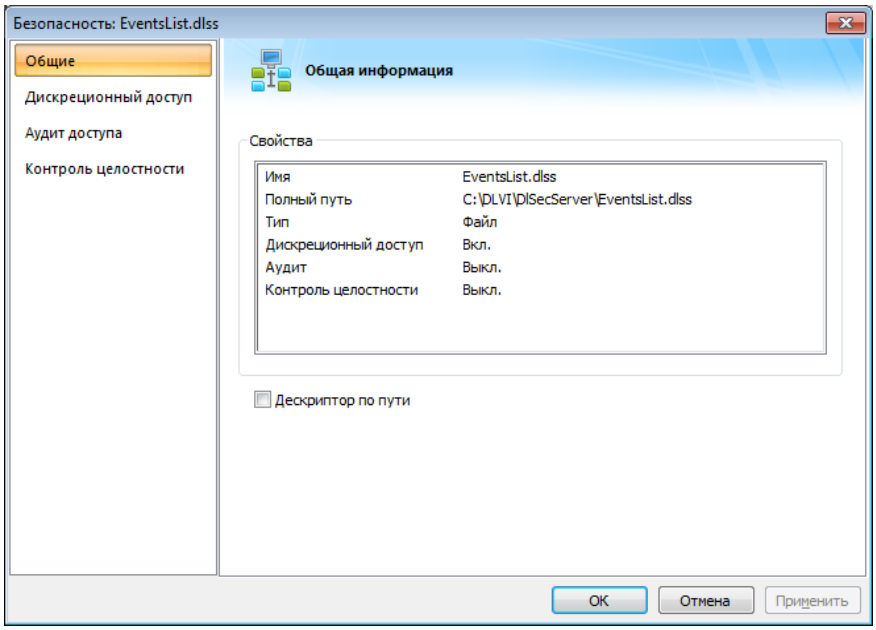


Рис. 192 – Дескриптор объекта ФС

Окно дескриптора состоит из закладок: «Общие», «Дискреционный доступ», «Аудит», «Контроль целостности». В зависимости от объекта тот или иной дескриптор доступа может отсутствовать, как и соответствующая ему закладка.

Окно дескриптора можно вызвать на уровне Сервера УД, группы или клиента на вкладке «Контроль ресурсов» через контекстное меню объекта либо нажав кнопку свойства в категории «Действия».

Для одновременно выделенных нескольких объектов в открывшемся окне дескриптора будут просматриваться установленные параметры безопасности всех объектов: причем, на закладке «Общие» параметры будут перечислены списком, на других закладках будет иметь место различное состояние (вид) отмеченных параметров:

 — отмеченное флажком поле означает, что данное свойство включено для всех выделенных объектов.

 — затемненное поле означает неопределенность: свойство включено для одних и выключено на других объектов.

 — пустое поле означает, что свойство выключено для всех выделенных объектов.

6.1.2 Дискреционный доступ

В СЗИ ВИ реализован собственный механизм дискреционного доступа. Данный механизм основывается на предоставлении пользователю прав на определенные операции с объектами файловой системы. Этот способ разграничения доступа похож на NTFS в Windows, но не зависит от него. Благодаря этому, права доступа СЗИ ВИ могут быть назначены не только на диски отформатированные под NTFS, но и на диски с другими файловыми системами, сменные накопители, сетевые ресурсы. При этом СЗИ ВИ не заменяет встроенный механизм NTFS, а дублирует его. То есть одновременно работают оба механизма, и чтобы пользователь получил доступ к объекту, СЗИ ВИ и NTFS должны разрешить доступ. Если же хоть один из этих механизмов откажет в доступе, пользователь не сможет работать с объектом ФС.

Примечание. При возникновении ситуации, в которой в СЗИ ВИ доступ к объекту разрешен, но фактически доступа нет, то в первую очередь следует проверить, какие права NTFS установлены на этот объект. Данную ситуацию легко отследить, если на объект назначить аудит отказов доступа. В случае, если доступ будет блокироваться NTFS, а также включен параметр «Аудит доступа: Заносить в журналы ошибки Windows» (на уровне Сервера УД «Параметры безопасности домена» → «Аудит»), то в журнале напротив записи будет отображен особый значок – с буквой «w», а если доступ блокируется установленной системой защиты – то стандартный значок отказа.

По умолчанию в СЗИ ВИ все пользователи имеют доступ ко всем объектам.

Рекомендуется при использовании СЗИ ВИ, разграничивать доступ к файловой системе только средствами СЗИ ВИ, а механизм разграничения доступа NTFS не использовать.

6.1.2.1 Права доступа

Применительно к правам доступа, всех пользователей, зарегистрированных в системе защиты, можно разделить на 4 вида:

1. **Учетные записи.** Это индивидуальные учетные записи пользователей, для которых установлены индивидуальные (отличные от других пользователей и групп пользователей) права доступа, а также учетные записи, зарегистрированные по маске для доменных пользователей.
2. **Группы пользователей**. Всем пользователями, входящим в одну группу, автоматически назначаются права на доступ, установленные для группы.
3. **Все.** К этому виду относятся все пользователи, для которых не установлены индивидуальные права доступа и одновременно не входящие ни в одну из групп. Такие пользователи автоматически объединяются в группу «Все». Этой группе, как и любой другой, могут быть разрешены/запрещены любые операции с любыми объектами файловой системы.
4. **Системные пользователи.** Данные пользователи не включены в вид пользователей «Все». Неосторожные блокировки для системных пользователей могут привести к неправоспособности системы.

В СЗИ ВИ каждому объекту ФС может быть сопоставлен список, элементами которого могут являться индивидуальные пользователи, учетные записи «по маске», группы пользователей и разряд «Все».

Каждый объект системы защиты характеризуется набором параметров безопасности. Каждый параметр безопасности контролирует определенную операцию (удаление, выполнение, изменение и другие), которая может быть произведена с объектом. Любая операция с объектом может быть разрешена либо запрещена пользователю. Соответственно каждый параметр может иметь значение «разрешить» или «запретить» (флажки в соответствующих полях).

Права доступа можно задавать либо для индивидуальной учетной записи пользователя, либо для группы, либо для учетной записи пользователя «по маске».

Операции, которые можно производить с объектами в СЗИ ВИ на уровне домена (Сервера УД) и группы, зависят от типа объектов:

- **Локальные диски и сменные накопители:**
  - **Обзор папки. Чтение содержимого**. Позволяет увидеть все вложенные в данную папку каталоги, подкаталоги, файлы, содержащиеся в корневом каталоге объекта.
  - **Изменение содержимого.** Изменение находящихся в папке вложенных папок и файлов (запись, удаление, создание).
  - **Удаление вложенных объектов.**
  - **Выполнение вложенных объектов.** Выполнение находящихся в папке соответствующих файлов.
  - **Чтение разрешений.** Просмотр значения параметров безопасности, установленных для ресурса.
  - **Запись разрешений.** Просмотр и редактирование параметров безопасности, установленных для ресурса.
  - **Низкоуровневое чтение.** Просмотр содержимого диска используя прямой доступ к диску.
  - **Низкоуровневая запись.** Удаление файлов с диска, а также запись на диск модифицированного (измененного) файла, используя прямой доступ к диску.
- **Удаленные диски, каталоги и подкаталоги (папки и подпапки):**
  - **Обзор папки. Чтение содержимого**. Позволяет увидеть все вложенные в данную папку каталоги, подкаталоги, файлы, содержащиеся в корневом каталоге объекта.
  - **Изменение содержимого.** Изменение находящихся в папке вложенных папок и файлов (запись, удаление, создание).
  - **Удаление вложенных объектов.**
  - **Выполнение вложенных объектов.** Выполнение находящихся в папке соответствующих файлов.
- **Файлы (могут находиться на локальных дисках, на сменных носителях, на сетевых ресурсах):**
  - **Чтение**. Просмотр содержимое файла любого типа.
  - **Запись.** Удаление файлов, а также запись на диск модифицированного (измененного) файла.
  - **Удаление.**
  - **Выполнение**. Имеет смысл только для программ. Позволяет запускать программу на выполнение.

- **Дополнительные параметры для файлов и папок:**
  - **Чтение разрешений.** Просмотр значения параметров безопасности, установленных для ресурса.
  - **Изменение разрешений**. Просмотр и редактирование параметров безопасности, установленных для ресурса.
- **Ветки реестра:**
  - **Чтение.** Позволяет прочитать содержимое.
  - **Запись.** Создание и удаление параметров в ветке реестра и ее самой.
  - **Удаление.**
  - **Чтение разрешений.** Просмотр значения параметров безопасности, установленных для ресурса.
  - **Запись разрешений.** Просмотр и редактирование параметров безопасности, установленных для ресурса.

Если объект является вложенным, и ему не сопоставлен список пользователей с правами, то права доступа пользователя к данному объекту определяются параметрами корневого объекта.

Если пользователь находится в сопоставленном объекту списке и одновременно входит в состав группы пользователей, находящейся в сопоставленном объекту списке, то действуют параметры доступа, установленные для этого пользователя.

Если пользователь входит в состав нескольких групп, находящихся в сопоставленном объекту списке, и хотя бы для одной из этих групп установлен запрет на совершение данной операции, а также отсутствует индивидуальное сопоставление данного пользователя объекту (нет явно назначенных прав), то пользователю эта операция запрещена.

Если пользователь не находится в сопоставленном объекту списке и не входит ни в одну из сопоставленных объекту (или корневому объекту) групп пользователей, то для него действуют параметры, установленные для группы «Все».

Примечание. Если для какого-то объекта назначить параметры безопасности (права доступа, аудит или контроль целостности) и этот ресурс переименовать, то параметры безопасности сохранятся (за исключением случая назначения дескрипторов для пути, подробнее в п. 6.1.3 «Дескрипторы по пути»).

Примечание. Если сделать копию объекта файловой системы, на который назначены параметры безопасности, то копия не будет иметь таких же параметров безопасности.

6.1.2.2 Механизм определения прав доступа пользователя к ресурсам ФС

При попытке пользователя совершить с объектом файловой системы компьютера любую операцию СЗИ ВИ анализирует назначенные права доступа согласно иерархии назначенных параметров на объекты снизу-вверх, то есть проверка происходит, начиная с локальных параметров объекта; глобальные параметры проверяются в последнюю очередь. При этом локальные настройки имеют приоритет над глобальными настройками.

Причем при проверке прав дискреционного доступа назначенные права прибавляются. Это означает, что происходит проверка значения (наличие флажков «запретить»/«разрешить») для каждого наименования прав (обзор, выполнение, чтение, запись и пр.), и, если право не имеет состояния «запретить»/«разрешить» на нижнем уровне, то система проводит проверку и присваивает значение состоянию, исходя из более высокого уровня параметров, к которому относится данный объект.

Если право имеет различные состояния «запретить»/«разрешить» на разных уровнях, например, «запретить» для файла и «разрешить» для более глобального уровня, папки, в которую вложен файл, то приоритетным будет право локального уровня «запретить».

Приоритеты параметров в СЗИ ВИ представляют собой следующую иерархию:

Таблица 2. Приоритеты параметров дескрипторов

Тип параметров	Название параметра	Приоритет
Локальные параметры	Параметры файлов	**Самый высокий**

	Параметры конкретных экземпляров накопителей	
	Параметры отдельных веток реестра	
	Параметры папок (приоритет меняется в зависимости от иерархии папок)	**Высокий**
Глобальные параметры **(список глобальных параметров на вкладке «Контроль ресурсов» → «Глобальные»)**	«Параметры CD-ROM дисков по умолчанию» «Параметры открытых USB-Flash дисков по умолчанию» «Параметры открытых FDD-дисков по умолчанию»	**Средний**
	«Параметры открытых сменных накопителей по умолчанию» «Параметры фиксированных дисков по умолчанию» «Параметры сети по умолчанию» «Параметры реестра по умолчанию»	**Низкий**
	«Параметры ФС по умолчанию»	**Самый низкий**

В системе защиты реализован механизм назначения дискреционных прав как на глобальные параметры (п. 6.1.2.3 «Дискреционный доступ для глобальных параметров», так и на локальные объекты файловой системы (п. 6.1.2.4 «Дискреционный доступ для локальных объектов ФС и веток реестра на клиентах»).

Таким образом, система защиты последовательно выполняет следующие действия проверки:

1. Если для данного объекта ФС пользователю назначены права, то возможность совершения запрошенной операции устанавливается исходя из этих прав. Если параметру, контролирующему данную операцию, присвоено значение «Разрешить», то операция выполняется. Если параметру присвоено значение «Запретить», операция блокируется.
2. Если для данного объекта ФС не назначены права для данного пользователя, но права назначены для одной из групп, в которую входит пользователь, то для определения возможности совершения запрашиваемой операции аналогично используются права этой группы.
3. Если для данного объекта ФС не назначены права ни конкретно для данного пользователя, ни для какой-либо из групп, в которые входит этот пользователь, то для определения возможности совершения запрошенной операции используются права, назначенные группе «Все».
4. Если же права не назначены ни для пользователя, ни для какой-либо группы, куда этот пользователь входит, ни для группы «Все», то система защиты проверяет, входит ли данный объект в состав другого объекта (папка/диск). Если входит, то повторяются действия 1-3 для объекта, содержащего данный объект. Если объект не входит в состав другого объекта ФС, то система защиты переходит к проверке глобальных параметров по иерархии, представленной в таблице.
5. Анализ глобальных параметров осуществляется по той же самой схеме, что и локальных на клиентах. Проверяются права, назначенные для пользователя, если они не назначены, то для групп, куда этот пользователь входит, и если права не назначены для таких групп, то проверяются права группы «Все». Если же и для группы «Все» не назначены права, то аналогично проверяются права глобальных параметров, имеющих более низкий приоритет. Если осуществлялась проверка глобальных параметров самого низкого приоритета, то выполнение операции разрешается.

Пример

Пусть существует файл, расположенный по пути «C:\Docs\balans.txt». Также есть следующие пользователи, каждый из которых входит только в одну группу:

- «Оператор», в группе «Пользователи»;
- «Аудитор», в группе «Пользователи»;
- «Админ», в группе «Администраторы».

На файл «C:\Docs\balans.txt» назначены права:

- группа «Все» – доступ запрещен;
- группа «Пользователи» – разрешено чтение;
- пользователь «Оператор» – разрешен полный доступ.

В результате распределения системой прав на данный объект, пользователи будут иметь следующие возможности для совершения операций с объектом:

- пользователь «Оператор» будет иметь полный доступ к файлу «C:\Docs\balans.txt» (права для пользователя будут проверяться первыми, и они имеют более высокий приоритет, чем права, заданные для групп);
- пользователь «Аудитор» будет иметь доступ только на чтение (для него не назначено отдельных прав, но он входит в группу «Пользователи»);
- пользователь «Админ» не получит доступа к этому файлу (для него не назначено отдельных прав, он не входит в группу «Пользователи», поэтому для него будут использоваться права, назначенные для группы «Все»).

6.1.2.3 Дискреционный доступ для глобальных параметров

Список глобальных параметров ФС расположен на уровне Сервера УД на вкладке «Контроль ресурсов домена» → «Глобальные» (рис. 193) и на уровне группы на вкладке «Контроль ресурсов группы» → «Глобальные» (рис. 194).

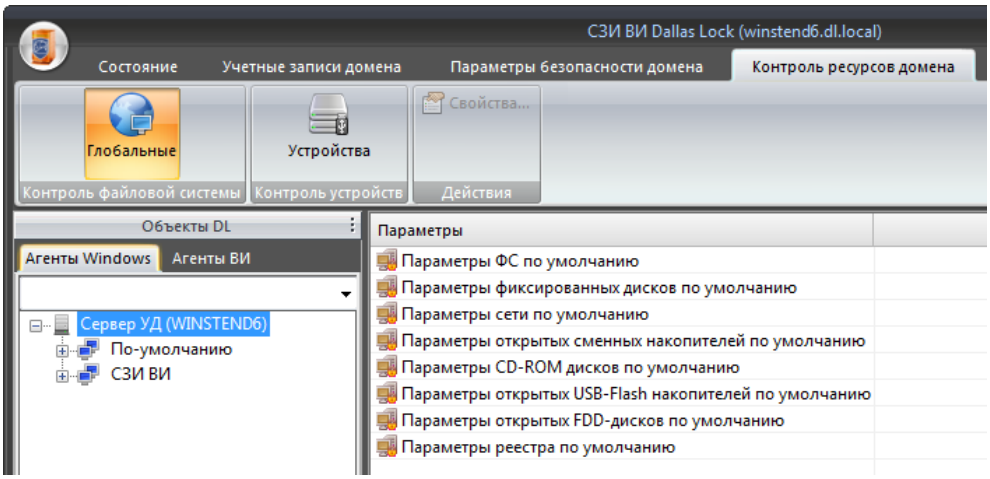


Рис. 193 – Назначение глобальных параметров безопасности домена

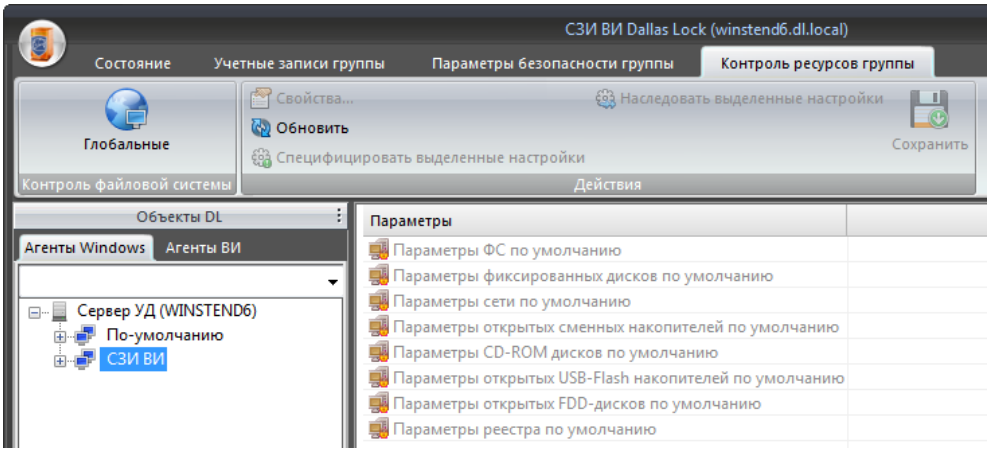


Рис. 194 – Назначение глобальных параметров безопасности группы

Глобально права дискреционного доступа можно назначить:

Таблица 3. Глобальные дескрипторы

Назначение	Название параметра в СЗИ ВИ Dallas Lock
на все ресурсы файловой системы	«Параметры ФС по умолчанию»
на жесткие диски, в том числе на устройства типа внешний жесткий диск USB	«Параметры фиксированных дисков по умолчанию»
на все сетевые ресурсы	«Параметры сети по умолчанию»
на все типы сменных накопителей, которые не были преобразованы, кроме CD-ROM дисков (по	«Параметры открытых сменных дисков по умолчанию»

умолчанию)	
на все приводы компакт-дисков на данном компьютере	«Параметры CD-ROM дисков по умолчанию»
на все сменные накопители типа USB-Flash носителей, которые не были преобразованы (по умолчанию)	«Параметры открытых USB-Flash носителей по умолчанию»
на все Floppy-диски на данном компьютере, которые не были преобразованы (по умолчанию)	«Параметры открытых FDD-дисков по умолчанию»
для всего реестра	«Параметры реестра по умолчанию»

Чтобы установить дискреционный доступ, необходимо выделить параметр и нажать кнопку «Свойства» на панели действий. Откроется окно редактирования параметров безопасности – дескриптор объекта, в котором необходимо выбрать закладку «Дискреционный доступ» (рис. 195).

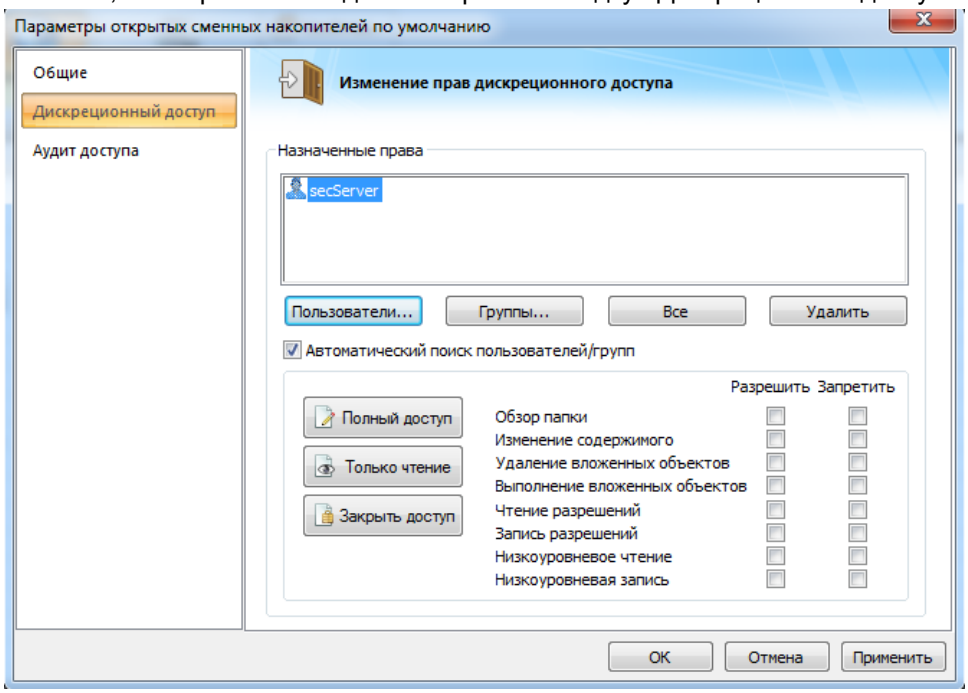


Рис. 195 – Назначение прав дискреционного доступа

Чтобы назначить определенные дискреционные права для пользователей, необходимо:

1. Выбрать определенные учетные записи пользователей или групп. После нажатия кнопок «Пользователи или «Группы» появятся типовые диалоговые окна с возможностью поиска учетных записей. Для выбора доменных учетных записей в поле «Размещение» необходимо выбрать имя домена, после чего появится список всех доменных учетных записей, зарегистрированные в СЗИ ВИ будут выделены особенным образом.
2. Для каждой учетной записи, пользователя или группы в списке необходимо задать набор разрешений/запретов, который будет определять права по доступу к данному объекту файловой системы (рис. 196).

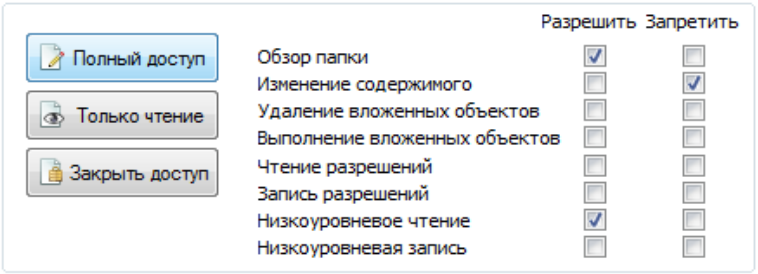


Рис. 196 – Список прав дискреционного доступа

3. Далее нажать кнопки «Применить» и «ОК».

Примечание. Если в процессе назначения запрета на чтение на CD-ROM диски выполняется подключения CD-ROM диска, данные права в зависимости от скорости монтирования диска могут не отработать. Соответственно, назначение прав на CD-ROM диски и эксплуатирование СЗИ ВИ в части контроля за данными типами носителей следует разносить во времени хотя бы несколько десятков секунд.

6.1.2.4 Дискреционный доступ для локальных объектов ФС и веток реестра на клиентах

Для того чтобы назначить дискреционный доступ для конкретного объекта ФС или ветки реестра на клиенте необходимо выполнить следующее:

1. Убедиться, что клиент подключен к Серверу УД. Если это не так, то следует подключить клиент («Состояние» → «Основное» → «Действия с клиентом» → «Подключиться»).
2. Перейти на вкладку «Контроль ресурсов», перейти в категорию «Доступ», выбрать объект ФС или путь реестра из списка и в категории «Действия», либо через контекстное меню, нажать кнопку «Свойства». Для добавления нового объекта на вкладке «Контроль ресурсов» в меню действий выбрать «Добавить (ФС)» или «Добавить (Реестр)» (рис. 197).

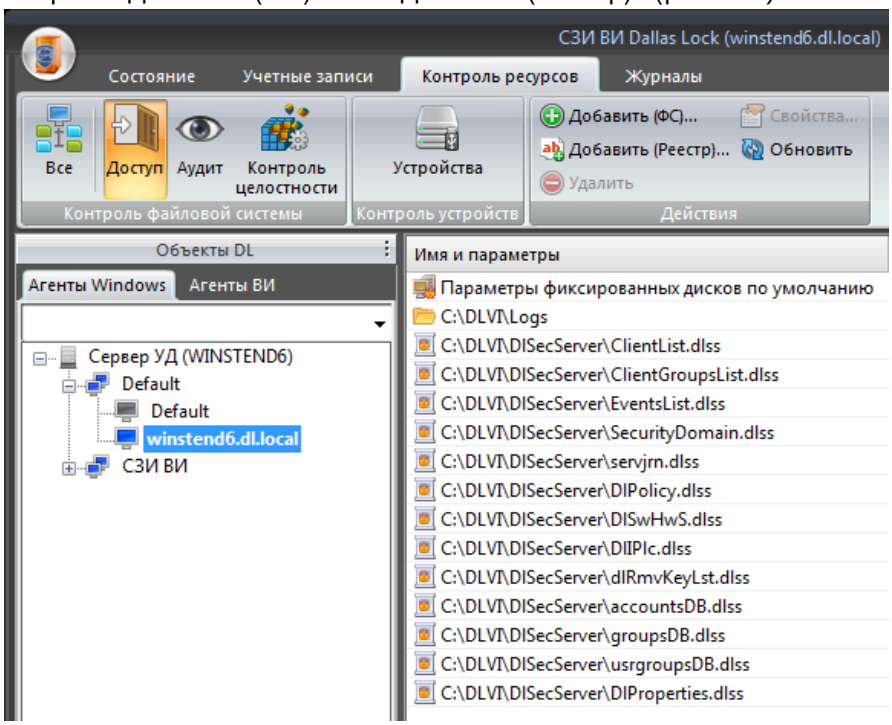


Рис. 197 – Окно дискреционного доступа

В появившемся окне проводника как в проводнике Windows необходимо найти нужный объект ФС и нажать кнопку «Выбрать» (рис. 198) или выбрать ветку реестра и нажать кнопку «Принять» (рис. 199). Для выбранного объекта откроется окно дескриптора.

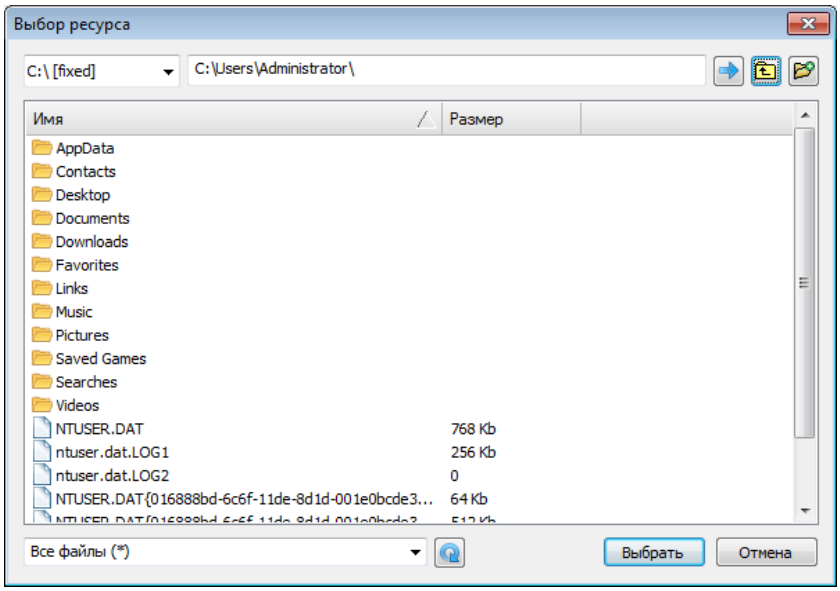


Рис. 198 – Окно выбора объекта ФС

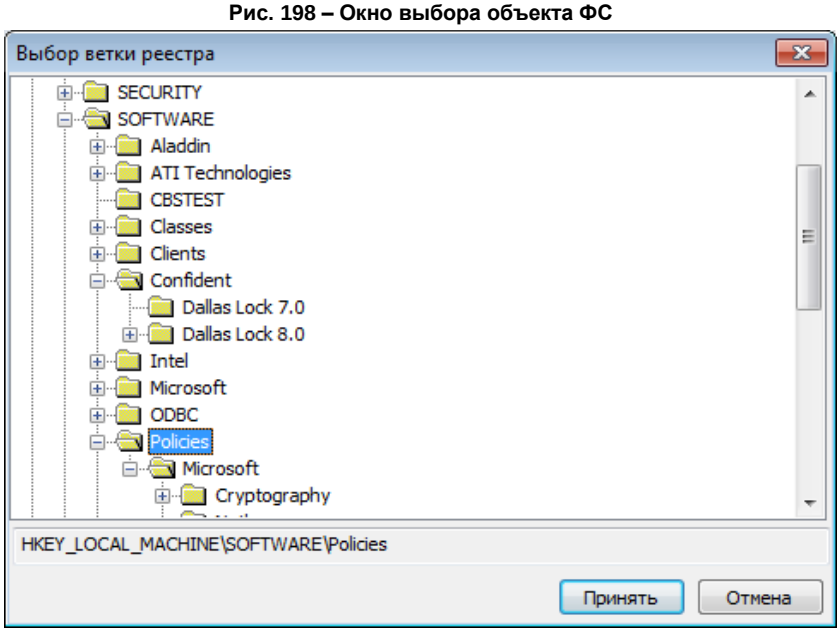


Рис. 199 – Окно выбора ветки реестра

3. В окне дескриптора безопасности необходимо выбрать закладку «Дискреционный доступ» (рис. 200).

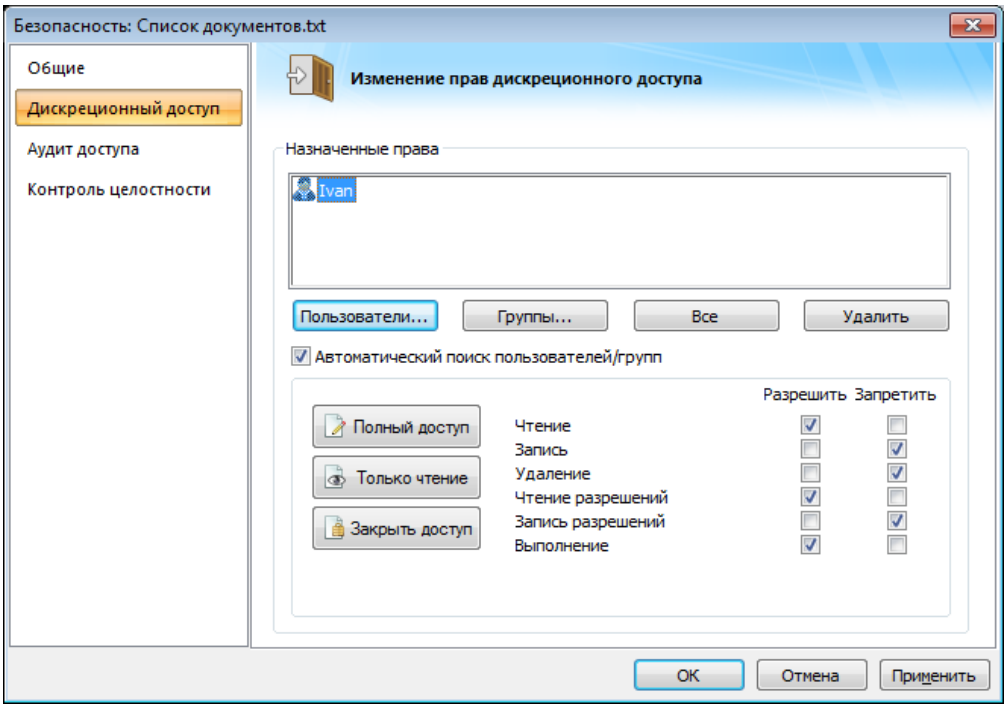


Рис. 200 – Назначение прав дискреционного доступа

В соответствии с дискреционным принципом доступа каждому ресурсу файловой системы может быть сопоставлен список пользователей и/или групп пользователей. Каждому пользователю (группе) из списка можно разрешить или запретить определенную операцию с данным ресурсом.

4. Чтобы назначить определенные дискреционные права для определенных пользователей необходимо при помощи кнопок «Пользователь», «Группы», «Все», «Удалить» выбрать определенные учетные записи пользователей или групп.
5. Для выбранных пользователей/групп необходимо задать набор разрешений/запретов, который будет определять права по доступу к данному объекту (рис. 201).

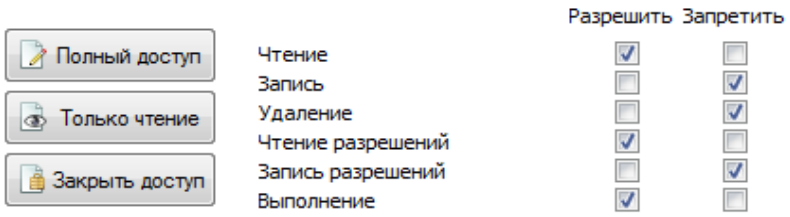


Рис. 201 – Список прав дискреционного доступа

Объекты, на которые назначен дискреционный доступ, автоматически появятся в списке объектов в окне категории «Дискреционный доступ» на вкладке «Контроль ресурсов».

При выборе категории «Все» на вкладке «Контроль ресурсов» также появится список, содержащий параметры всех объектов глобальных, локальных или сетевых на которые назначены какие-либо права доступа, а также контроль целостности и аудит.

Внимание! Введено ограничение в части назначения контроля целостности на защищаемые объекты размером свыше 5 Гб, поскольку это может сильно влиять на производительность работы СЗИ ВИ и привести к сбою в штатной работе СЗИ ВИ.

Права доступа к сетевым ресурсам

Подобно тому, как можно назначать права доступа на локальные ресурсы клиента, в СЗИ ВИ права доступа можно назначать и на сетевые ресурсы.

В этом качестве модель безопасности СЗИ ВИ отличается от модели безопасности, принятой в Windows.

Локально установленная ОС Windows контролирует только локальные ресурсы. СЗИ ВИ позволяет ограничивать доступ также и к сетевым ресурсам. Причем, если на удаленном компьютере, на который идет запрос, тоже установлена СЗИ ВИ, то права доступа будут проверяться два раза. Первый раз – локально установленной СЗИ ВИ перед тем, как запрос отправится в сеть, и второй

раз – удаленно установленной СЗИ ВИ, на которую придет запрос из сети.

Права доступа на сетевые ресурсы назначаются также, как и на локальные: необходимо ввести в форме поиска объекта полный сетевой путь.

При назначении доступа к сетевым ресурсам необходимо помнить следующее: фильтр файловой системы СЗИ ВИ, который отвечает за контроль доступа к файловой системе, получает путь к объекту в виде строки, которую он и анализирует. И если для локальных ресурсов в этом нет никаких проблем, то при работе с сетевыми ресурсами об этом нужно помнить, так как задать путь к одному и тому же сетевому ресурсу можно различными способами: используя имя компьютера, используя IP-адрес, используя IP-адрес в шестнадцатеричном виде и так далее.

Например, пусть имеется некоторый компьютер SERVER512 с IP-адресом 192.168.8.92, на котором расположена папка, открытая для общего доступа, с именем «sharedDocuments». Тогда пути «\\SERVER512\sharedDocuments\письмо.docx» и «\\192.168.8.92\sharedDocuments\письмо.docx» указывают на один и тот же документ.

Но с точки зрения Dallas Lock это разные пути, и поэтому, если назначены права на один из них, при обращении по другому пути, права действовать не будут.

Поэтому, если необходимо разграничить доступ к сетевым ресурсам для какого-либо пользователя, то нужно, обязательно, в глобальном дескрипторе «Параметры сети по умолчанию» (на уровне Сервера УД вкладка «Контроль ресурсов доменов» → категория «Глобальные», либо на уровне группы вкладка «Контроль ресурсов группы» → категория «Глобальные») запретить этому пользователю все действия и разрешить их для конкретных ресурсов. Иначе ограничения можно будет легко обойти.

6.1.2.5 Низкоуровневый доступ к диску и сменным накопителям

Если пользователю не разрешен низкоуровневый доступ к диску и сменным накопителям, то он не сможет запускать программы, использующие прямой доступ к данными носителями информации на защищенном компьютере. Тем самым обеспечивается предотвращение несанкционированного доступа к информации и к работе с данными носителями информации при помощи таких программ.

Под сменными накопителями подразумеваются те устройства, которые распознаются ОС как сменный/съемный (removable). Это USB-Flash накопители, карты памяти, floppy- и компакт-диски и прочие.

Жесткие диски, подключаемые через устройство Mobile Rack или USB-порт, физически являются сменными, но логически, для ОС, являются фиксированными.

Для того чтобы назначить дискреционные права на низкоуровневый доступ к диску или сменному накопителю, необходимо установить соответствующий набор разрешений/запретов для дескриптора или глобального параметра (рис. 202).

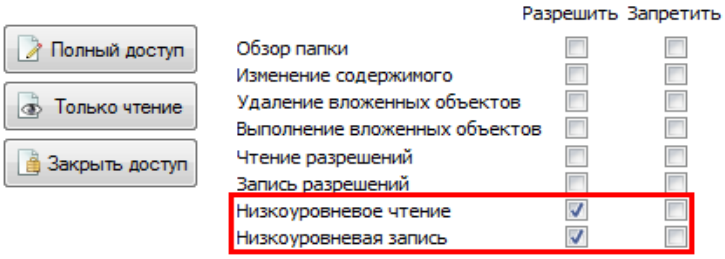


Рис. 202 – Список прав дискреционного доступа

6.1.3 Дескрипторы по пути

Как отмечалось выше, если на объект файловой системы установлен дескриптор, то при переименовании этого объекта, дескриптор останется на нем. Если удалить объект – дескриптор удалится тоже. То есть дескриптор «привязан» к объекту.

Но, в редких случаях это бывает неудобно. Например, при работе с Microsoft Word. Программа MS Word устроена таким образом, что когда в ней открывается какой-либо документ, после редактирования и сохранения изменений, она выполняет последовательность следующих действий:

- переименовывает исходный документ;
- создает новый документ под первоначальным именем;
- удаляет переименованный исходный документ.

Что происходит с дескриптором, если он назначен на документ, при его редактировании? Он переименовывается и удаляется вместе с исходным документом. СЗИ ВИ исправно работает в соответствии с заложенными в ней принципами. Но для пользователя же это выглядит как ошибка: на документ были назначены права, пользователь его отредактировал, права исчезли. Возникает

противоречивая ситуация.

Чтобы таких ситуаций не возникало, самое правильное – назначать права не на документы, а на папки, в которых эти документы находятся.

Но это бывает неудобно, например, когда в одной папке должны лежать несколько документов с разными правами. В этом случае на эти документы нужно назначать дескрипторы по пути. Их отличие от обычных дескрипторов в том, что они не переименовываются и не удаляются вместе с объектом. Они «привязаны» к конкретному пути и могут существовать даже, если по этому пути никаких документов не находится.

Для того чтобы создать дескриптор по пути, нужно в окне редактирования параметров объекта на вкладке «Общие» установить флаг в поле «Дескриптор по пути» (рис. 203).

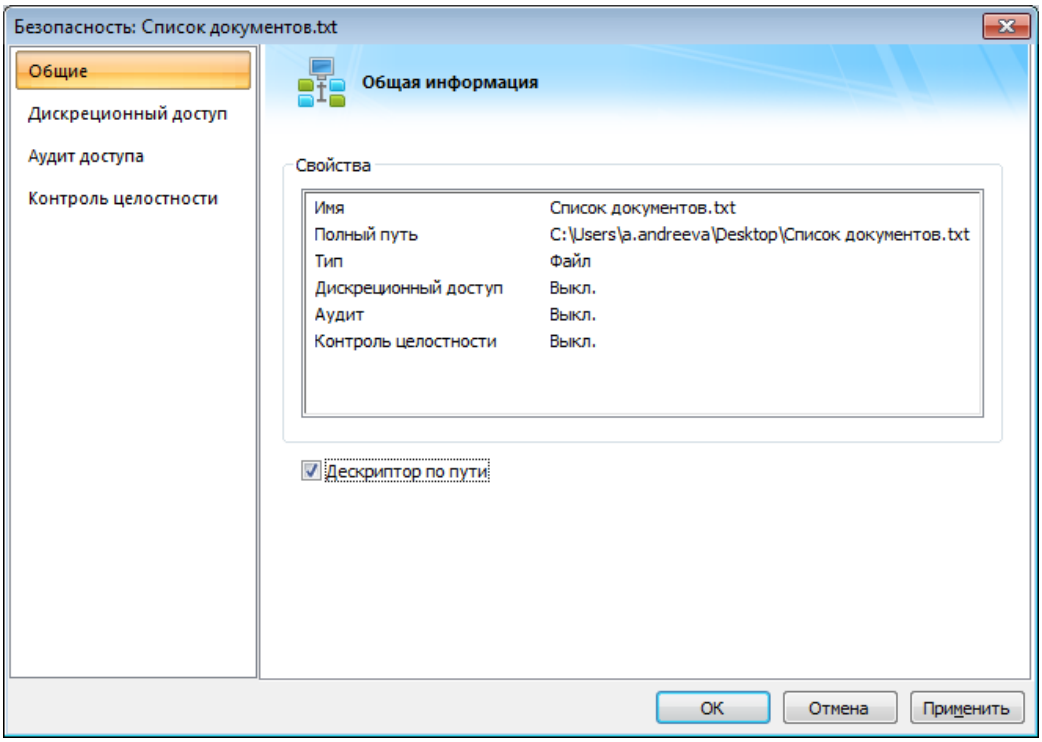


Рис. 203 – Назначенный дескриптор по пути

Дескрипторы по пути выделены в списке контролируемых объектов голубым значком  , обычные дескрипторы имеют белый значок, глобальные – оранжевый, дескрипторы папок имеют значок в виде папки, дескрипторы сетевых ресурсов и веток реестра также отличаются.

Без лишней необходимости использовать дескрипторы по пути не рекомендуется.

6.2 Контроль устройств в ОС Windows

Основной задачей функции контроля доступа к устройствам в СЗИ ВИ является возможность разграничения доступа к подключаемым на ПК устройствам для определенных пользователей или групп пользователей и ведения аудита событий данного доступа.

Разграничение доступа и ведение аудита возможно, как для классов устройств, так и для конкретных экземпляров. К классу устройств на конкретном ПК может быть одновременно отнесено одно, несколько или ни одного устройства.

Чтобы произвести настройки доступа для контроля устройств, необходимо в дереве «Агенты Windows» на основной вкладке главного меню «Контроль ресурсов» выбрать категорию «Контроль устройств» (рис. 204).

В основном окне отобразится дерево устройств, которое состоит из двух уровней иерархии: классов и индивидуальных устройств, которые входят в определенный класс. Если в класс входит несколько устройств, они отображаются последовательно.

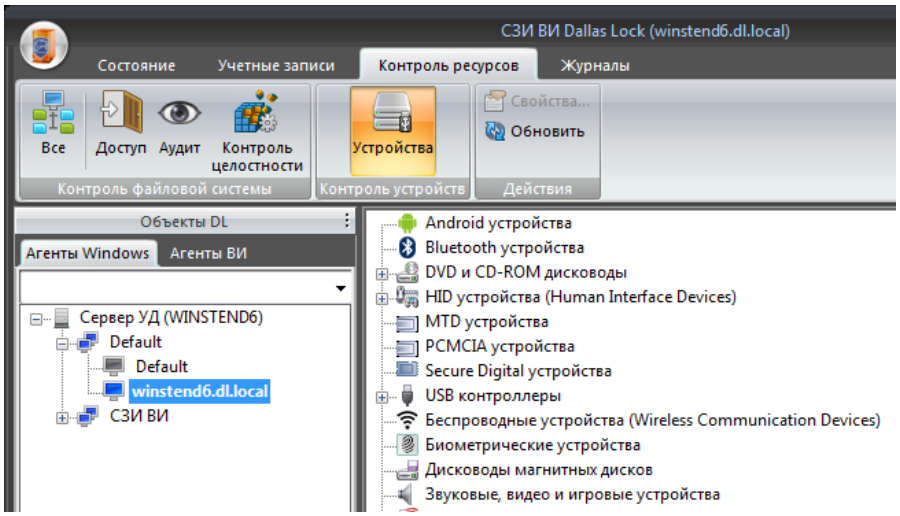


Рис. 204 – Дерево классов и видов устройств

Список классов в СЗИ ВИ фиксирован и одинаков для всех защищенных ПК. Список устройств на каждом ПК свой индивидуальный, он берется из локальной операционной системы.

Также возможно блокировать перенаправляемые по RDP протоколу (Remote Desktop Protocol) устройства.

Примечание. Часть устройств ПК относится к системным, без которых работа компьютера невозможна (процессора, оперативная память, видеоадаптеры, мосты системной платы и т.д.). Разграничивать доступ к таким устройствам не имеет смысла, т.к. запрет доступа к ним приведет к тому, что пользователь не сможет загрузить систему. Поэтому СЗИ ВИ такие устройства не контролирует.

Примечание. При настройке работы с USB-устройствами их можно подключать как напрямую через USB-порт, так и через интерфейсные модули типа Anywhere USB.

6.2.1 Разграничение доступа к устройствам

При настройке разграничения доступа к устройствам необходимо учесть следующие особенности:

1. В разных версиях ОС Windows в диспетчере устройств одно и то же физическое устройство может идентифицироваться по-разному. Это следует учитывать при определении прав доступа к устройству/классу устройств, особенно при централизованной настройке средствами ЦУ СЗИ ВИ.
   Мобильные телефоны в зависимости от комплектации самого устройства могут определяться как беспроводное устройство, как USB-Flash накопитель, как набор портов, или даже как несколько устройств одновременно. В категорию «Беспроводные устройства» могут попадать устройства беспроводного доступа, такие как современные мобильные телефоны-модемы, в тоже время беспроводные адаптеры WiFi обычно попадают в категорию «Сетевые адаптеры». Это связано с особенностью реализации самих устройств и их драйверов, и может быть установлено наверняка опытным путем.
2. Иногда некоторые устройства после их выключения могут потребовать перезагрузку компьютера для последующего включения. Это особенность конкретных устройств, которая будет проявляться и без СЗИ ВИ (если, например, вручную запретить устройство через диспетчера устройств).
3. При разграничении доступа к устройствам, отличным от COM/LPT-портов, запрет доступа действует на всех пользователей и устройство полностью отключается в случае его запрета. Отключенное устройство будет недоступно, в том числе, для учетной записи пользователя, выполнившего установку СЗИ ВИ.
4. Не рекомендуется глобально запрещать все USB-контроллеры, лучше выполнять блокировку на уровне конкретных контроллеров и устройств.
5. Запрещая использование некоторых устройств, например, USB-устройств ввода, можно лишиться возможности работать устройствами типа «мышь» и «клавиатура».

Для настройки прав доступа к классам устройств или устройствам необходимо выбрать соответствующий элемент в дереве устройств и нажать на кнопку «Свойства» на панели действий (или выбрать данное действие в контекстном меню объекта).

Откроется окно редактирования дескриптора устройства, которое состоит из закладок: «Дискреционный доступ» и «Аудит доступа». В зависимости от политик безопасности необходимо выполнить установку прав доступа. Значки устройств и классов в дереве объектов, для которых назначены какие-либо права, будут выделены определенным образом.

6.2.1.1 Дискреционный доступ к устройствам

Дискреционный принцип разграничения доступа к устройствам состоит из двух возможностей: доступ всех пользователей к данному устройству разрешен и доступ запрещен (рис. 205). Для некоторых классов устройств разграничение дискреционного доступа на уровне пользователей не доступно, т.е. возможности выбора учетных записей нет, кроме записи «Все».

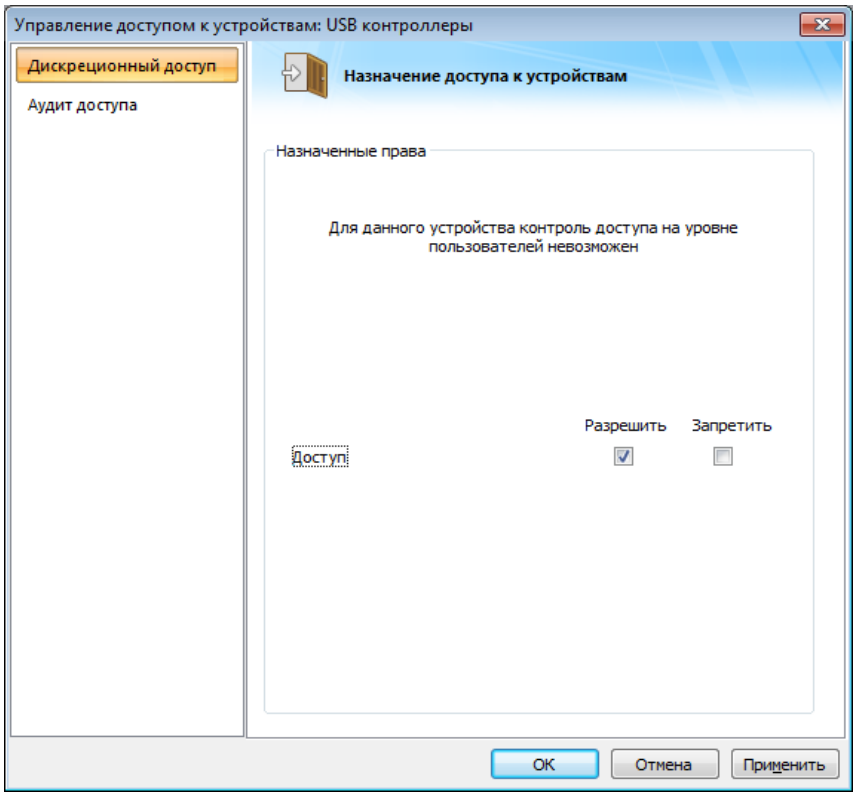


Рис. 205 – Дескриптор дискреционного доступа к устройству

Принцип определения прав доступа пользователей к устройствам аналогичен механизму определения прав доступа пользователя к ресурсам файловой системы (подробнее см. п. 6.1.2.2 «Механизм определения прав доступа пользователя к ресурсам ФС»):

1. Права, заданные для класса устройств, имеют более низкий приоритет, чем права, заданные для конкретного экземпляра.
2. Права, заданные для группы пользователей, имеют более низкий приоритет, чем права, заданные для пользователя (если доступно разграничение на уровне пользователей).
3. Если доступ к устройству не назначен ни классу, которому принадлежит устройство, ни самому устройству, то доступ разрешен.

6.2.2 Аудит доступа к устройствам

Для назначения аудита событий доступа к устройствам в первую очередь необходимо включить два глобальных параметра безопасности «Аудит устройств» и «Журнал ресурсов» на уровне Сервера УД на вкладке «Параметры безопасности» → «Аудит» (значение «Вкл.»).

В окне редактирования дескриптора выбранного устройства необходимо выбрать закладку «Аудит доступа». Далее включить аудит устройства: поставить флаг в поле «Аудит включен» и выбрать из двух событий аудита: аудит успешных подключений устройства («Успех») или аудит неуспешных подключений («Отказ»).

Если для конкретного устройства не установлен аудит событий, то события аудита будут соответствовать значениям для класса, которому принадлежит данное устройство; если у класса устройств тоже не будут выбраны значения аудита, то аудит вестись не будет.

Аудит событий доступа к устройствам, а также аудит событий по настройке доступа ведется в

журнале ресурсов (подробнее см. п. 9.2 «Аудит компьютеров клиентов Windows»).

6.3 Удаленный доступ к СВ

По умолчанию, после развертывания СЗИ ВИ, удаленное подключение к СВ доступно только с ЦУ СЗИ ВИ.

6.3.1 Правила управления СВ

Просмотр и редактирование списка правил управления СВ происходит на уровне СВ в категории «Состояние» → «Правила управления СВ» (рис. 206).

В правилах управления СВ задается список блокируемых портов и тип протокола (TCP/UDP) для удаленного подключения к СВ. По умолчанию заданы все стандартные порты, используемые для подключения к СВ.

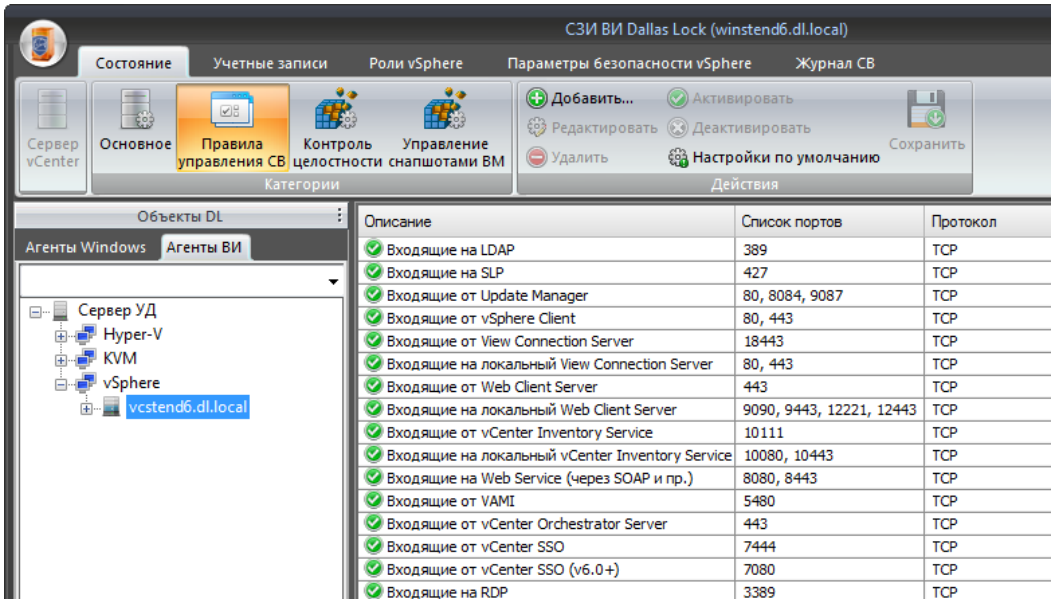


Рис. 206 – Правила управления СВ

Для того чтобы создать правило управления СВ необходимо:

1. Перейти на уровень СВ и открыть категорию «Состояние» → «Правила управления СВ».
2. Нажать кнопку «Добавить».
3. Для того, чтобы изменить описание, задать список портов и тип протокола для правила, нужно щелкнуть по ним два раза левой кнопкой мыши либо в категории «Действия» нажать кнопку «Редактировать» и ввести новые значения.
4. Далее следует нажать кнопку «Сохранить».
5. Открыть вкладку «Состояние» и нажать кнопку «Синхронизировать».
   Для того, чтобы деактивировать правило необходимо выделить это правило и в категории «Действия» нажать кнопку «Деактивировать», а затем кнопку «Сохранить».

Чтобы отменить все изменения и вернуться к исходным настройкам правил, необходимо в категории «Действия» нажать кнопку «Настройки по умолчанию».

6.3.2 Клиенты управления СВ

Чтобы получить доступ к серверу виртуализации с удаленного компьютера, данный компьютер должен входить в список клиентов управления СВ.

Примечание. По умолчанию количество доверенных клиентов ограничено значением 512. Изменить максимальное количество доверенных клиентов можно в дополнительном меню Консоли в окне «Параметры сервера УД» в группе «VI CORE» в соответствующем пункте (см. п. 3.3.2 «Основные параметры работы ядра СЗИ ВИ» (рис. 89).

6.3.2.1 Клиенты управления СВ vSphere

Просмотр и редактирование списка клиентов управления vSphere происходит на уровне «vSphere» в категории «Состояние» → «Клиенты управления СВ» (рис. 207).

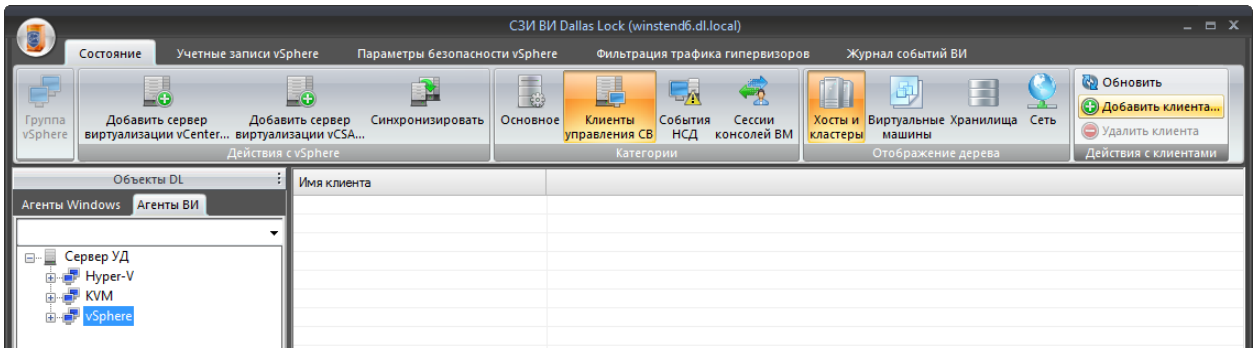


Рис. 207 – Клиенты управления СВ vSphere

Для того чтобы добавить клиента управления сервером виртуализации необходимо:

1. Выбрать уровень «vSphere» и открыть категорию «Состояние» → «Клиенты управления СВ».
2. Выбрать категорию «Действия с клиентами» и нажать кнопку «Добавить клиента».
3. В появившемся окне ввести имя в сети или IP-адрес клиента управления, после чего нажать кнопку «ОК».
4. Нажать кнопку «Синхронизировать».

6.3.2.2 Клиенты управления СВ Hyper-V

Просмотр и редактирование списка клиентов управления Hyper-V происходит на уровне «Hyper-V» в категории «Состояние» → «Клиенты управления СВ» (рис. 208).

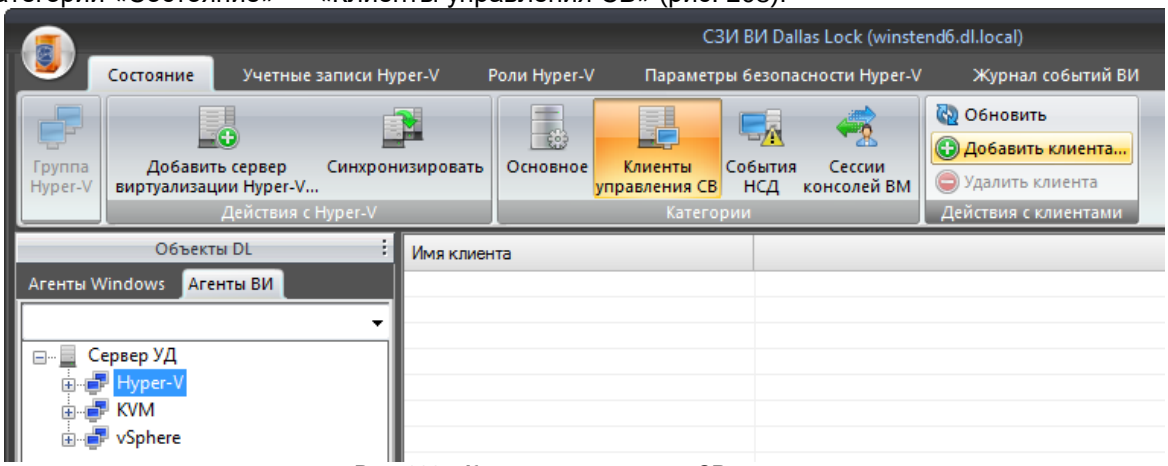


Рис. 208 – Клиенты управления СВ Hyper-V

Для того чтобы добавить клиента управления сервером виртуализации необходимо:

1. Выбрать уровень «Hyper-V» и открыть категорию «Состояние» → «Клиенты управления СВ».
2. В категории «Действия с клиентами» и нажать кнопку «Добавить клиента».
3. В появившемся окне ввести имя в сети или IP-адрес клиента управления, после чего нажать кнопку «ОК».
4. Нажать кнопку «Синхронизировать» в блоке «Действия с Hyper-V».

Внимание! В случае, если происходит блокировка какой-либо операции ВМ Hyper-V для пользователя с форматом имени «<домен>\<имя_СВ>$», то необходимо:

1. В дереве «Агенты ВИ» на уровне Hyper-V выбрать категорию «Клиенты управления СВ», нажать кнопку «Добавить клиента» в блоке «Действия с клиентами».
2. Указать имя клиента, в формате «<домен>\<имя_СВ>» (символ «$» не прописывается).
3. В появившемся диалоговом окне необходимо подтвердить продолжение операции, нажав кнопку «Да».
4. Нажать кнопку «Синхронизировать» в блоке «Действия с Hyper-V».
5. Дождаться окончания процедуры синхронизации и повторить операцию.

Клиенты управления СВ для ВМ Hyper-V

Взаимодействие между ВМ Hyper-V, работающих на отдельных гипервизорах, а также с ВМ, работающими на гипервизорах ESXi, возможно осуществлять путем добавления данных ВМ в список доверенных клиентов.
Для этого необходимо на уровне «Hyper-V» в категории «Состояние» → «Клиенты управления СВ» добавить ВМ в качестве клиента управления, указав при этом имя, либо IP-адрес ВМ, находящейся под управлением гипервизора. Эту процедуру необходимо произвести для всех ВМ, между которыми предполагается взаимодействие через порты, контролируемые СЗИ ВИ.

Внимание! Не рекомендуется удалять или деактивировать правила из списка блокируемых портов для удаленного подключения к СВ (подробнее см. п. 6.3.1 «Правила управления СВ», сформированного по умолчанию.

6.3.2.3 Клиенты управления СВ KVM/oVirt/zVirt/HOSTVM/РЕД Вирт

Просмотр и редактирование списка клиентов управления KVM происходит на уровне «KVM» в категории «Состояние» → «Клиенты управления СВ» (рис. 209)

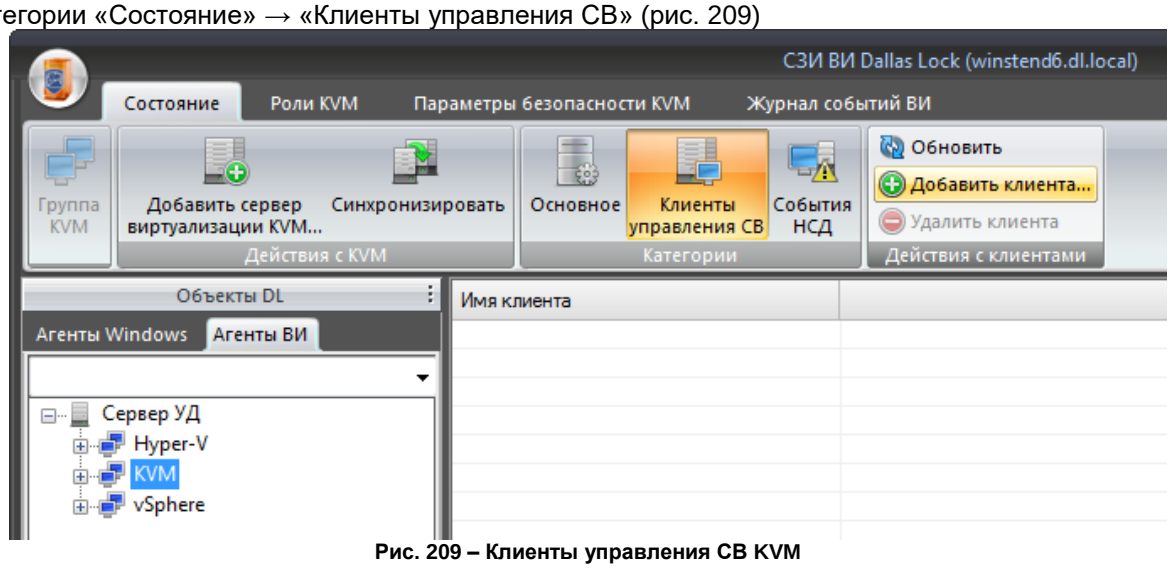


Рис. 209 – Клиенты управления СВ KVM

Для того чтобы добавить клиента управления сервером виртуализации необходимо:

1. Выбрать уровень «KVM» и открыть категорию «Состояние» → «Клиенты управления СВ».
2. В категории «Действия с клиентами» и нажать кнопку «Добавить клиента».
3. В появившемся окне ввести имя в сети или IP-адрес клиента управления, после чего нажать кнопку «ОК».
4. Нажать кнопку «Синхронизировать» в блоке «Действия с KVM».

6.4 Ролевая модель учетных записей СВ

Роль представляет собой совокупность привилегий — полномочий по выполнению действий в части администрирования СЗИ ВИ и ДБ. Для удобства привилегии группируются в несколько категорий в зависимости от области применения.

Различным субъектам доступа (учетным записям или группам пользователей) ДБ ставится в соответствие роль, отображающая права данного субъекта в части администрирования средствами СЗИ ВИ.

Для субъекта доступа (пользователя или группы) может быть назначена только одна роль на объект ВИ, однако, разрешения для пользователя могут складываться, если он является членом нескольких групп, для которых назначены разные роли на объект. При этом, если роль явно назначается для учетной записи пользователя, она перекрывает все права, полученные от групп. Однако если пользователь состоит хотя бы в одной группе, которой явно была назначена роль «Нет доступа», все привилегии считаются снятыми.

6.4.1 Ролевая модель учетных записей vSphere

Настройки по правам администрирования доступа к гипервизорам, объектам ВИ и виртуальным машинам vSphere осуществляются средствами ролевой модели разграничения доступа. Для просмотра и редактирования параметров ролевого доступа необходимо в дереве «Агенты ВИ» на

уровне группы vSphere перейти на вкладку «Роли vSphere» (рис. 210).

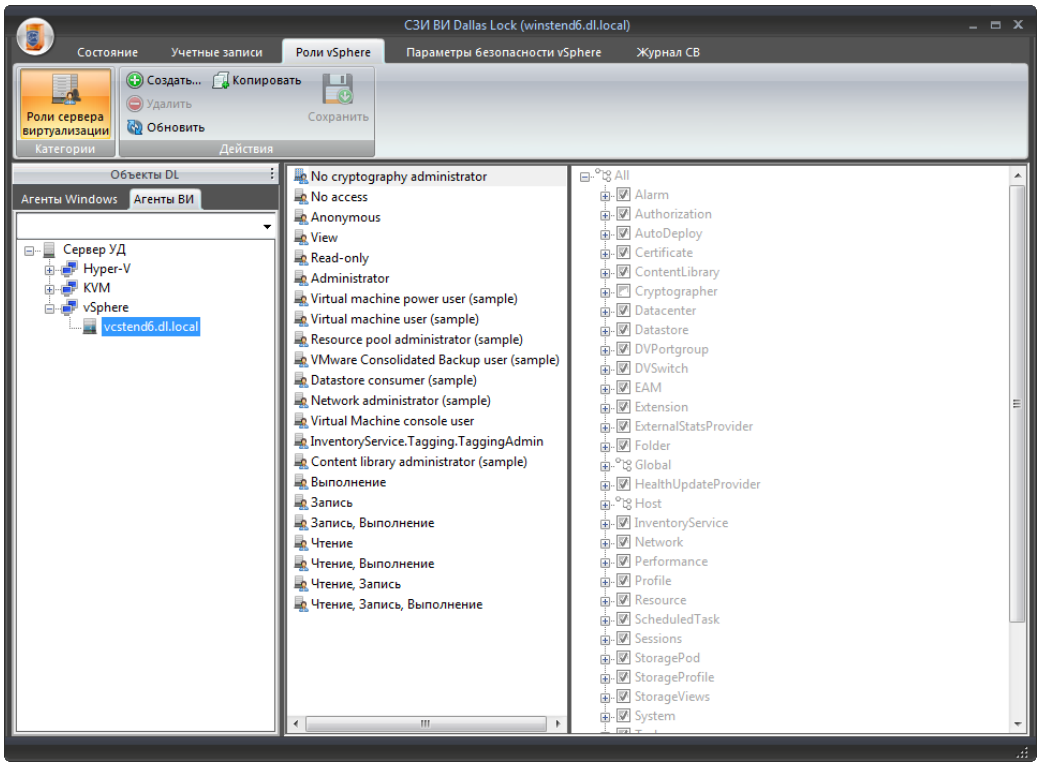


Рис. 210 – Роли сервера виртуализации vSphere

Внимание! Создавать и осуществлять настройку ролей может только суперадминистратор.

В группе vSphere на вкладке «Роли vSphere» присутствуют предустановленные роли, которые невозможно изменить (системные). Системные предустановленные роли, которые нельзя изменить или удалить, называются (Administrator, Read-only, No access).

Для системных ролей установлены следующие разрешающие привилегии:

- для роли «Administrator»: включены все привилегии;
- для роли «Read-only»: включена привилегия «System». Используется для аудита (только просмотр детальной информации и состояния объекта).
- для роли «No access»: все привилегии отключены.

Предустановленные роли, привилегии которых можно редактировать:

- Чтение;
- Запись;
- Выполнение;
- Чтение, Запись;
- Чтение, Выполнение;
- Запись, Выполнение;
- Чтение, Запись, Выполнение.

6.4.1.1 Создание и редактирование ролей vSphere

Для создания новой роли на СВ необходимо:

1. Выбрать уровень СВ и открыть вкладку «Роли vSphere» → «Роли серверов виртуализации».
2. Нажать кнопку «Создать», ввести имя для новой роли (рис. 211) и нажать клавишу «Enter» на клавиатуре.
3. Выбрать необходимые привилегии для роли и нажать кнопку «Сохранить» в блоке «Действия».
4. Открыть вкладку «Состояние» и нажать кнопку «Синхронизировать» или выбрать соответствующий пункт из контекстного меню (подробнее см. п. 3.5 «Синхронизация»).

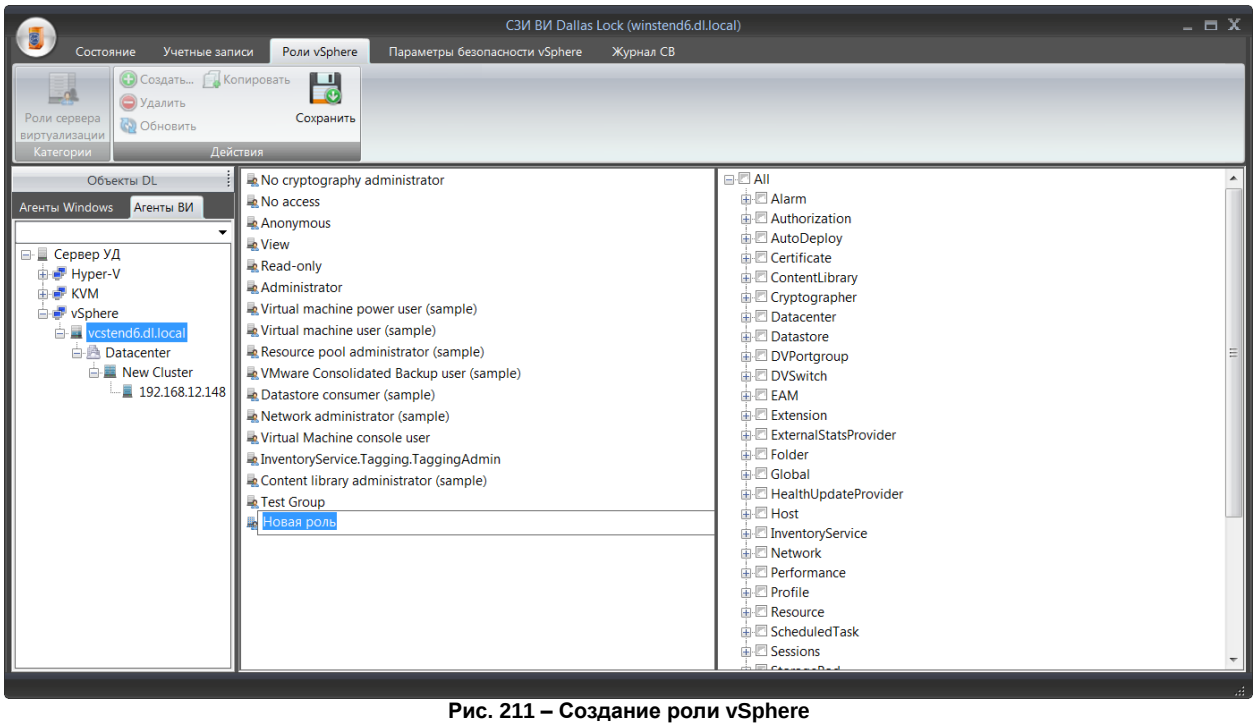


Рис. 211 – Создание роли vSphere

Все роли, за исключением системных ролей, можно переименовывать.

По умолчанию все привилегии для вновь созданных ролей отключены. Для назначения привилегий, необходимо корректно заполнить поле с привилегиями и нажать кнопку «Сохранить» в блоке «Действия».

После внесения всех необходимых изменений, следует выполнить сохранение путем нажатия кнопки «Сохранить» в блоке «Действия» и произвести синхронизацию (подробнее см. п. 3.5 «Синхронизация»).

6.4.1.2 Удаление ролей vSphere

Для удаления роли необходимо выделить роль, которую следует удалить и нажать кнопку «Удалить». При этом на экране появится предупреждение (рис. 212).

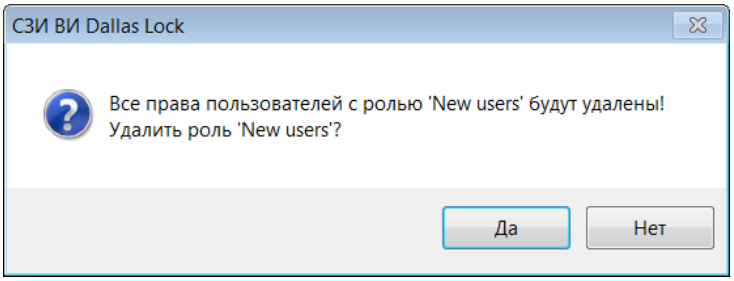


Рис. 212 – Удаление роли vSphere

После чего подтвердить операцию и произвести синхронизацию (подробнее см. п. 3.5 «Синхронизация»).

После удаления назначенной роли все назначения данной роли удаляются.

Для обновления списка ролей в категории «Действия» необходимо нажать кнопку «Обновить».

6.4.1.3 Управление ролями гипервизора ESXi

Порядок действий для ролей гипервизоров аналогичен п. 6.4.1.1, за исключением того, что все действия происходят на уровне гипервизора, во вкладке «Роли vSphere» → «Роли гипервизора (ESXi)» (рис. 213).

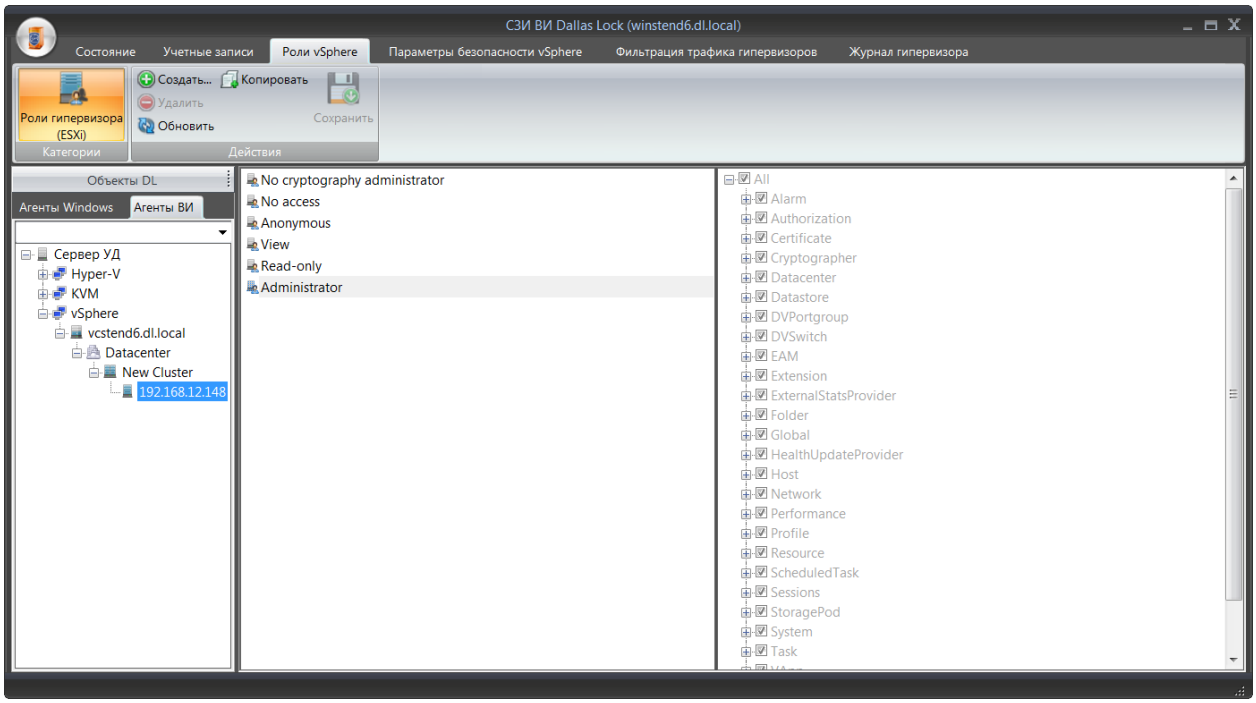


Рис. 213 – Роли гипервизора ESXi

6.4.2 Ролевая модель учетных записей Hyper-V

Настройки по правам администрирования доступа к гипервизорам, объектам ВИ и виртуальным машинам Microsoft Hyper-V осуществляются средствами ролевой модели разграничения доступа. Для просмотра и редактирования параметров ролевого доступа необходимо в дереве «Агенты ВИ» на уровне группы Hyper-V перейти на вкладку «Роли Hyper-V» (рис. 214).

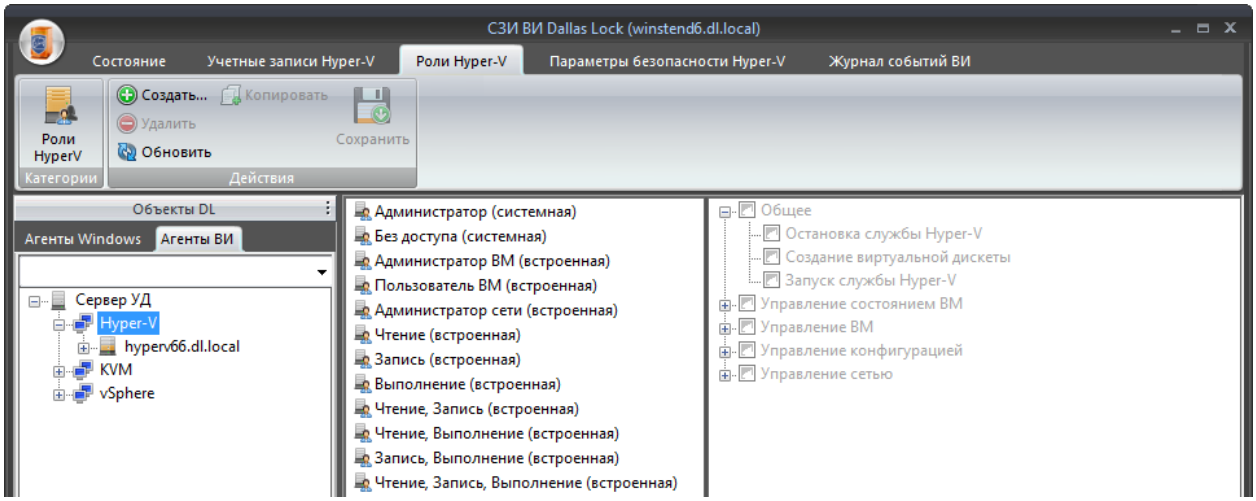


Рис. 214 – Роли Hyper-V

В дереве Hyper-V на вкладке «Роли Hyper-V» присутствуют предустановленные роли, которые невозможно изменить (системные), предустановленные роли, привилегии которых можно редактировать, а также существует возможность создания новых ролей.

Системные предустановленные роли, которые нельзя изменить или удалить, называются «Администратор» и «Без доступа».

Для системных ролей установлены следующие разрешающие привилегии:

- для роли «Администратор»: включены все привилегии;
- для роли «Без доступа»: все привилегии отключены.

Предустановленные роли, привилегии которых можно редактировать:

- Администратор ВМ;
- Пользователь ВМ;
- Администратор сети;
- Чтение;

- Запись;
- Выполнение;
- Чтение, Запись;
- Чтение, Выполнение;
- Запись, Выполнение;
- Чтение, Запись, Выполнение.

Также, следует учитывать, что редактирование ролей осуществляется на общем для всех СВ Hyper-V уровне, следовательно, на каждом СВ Hyper-V всегда создается одинаковый набор ролей.

6.4.2.1 Создание ролей Hyper-V

Для создания новой роли на СВ необходимо:

1. Выбрать уровень группы Hyper-V и открыть вкладку «Роли Hyper-V» → «Роли Hyper-V».
2. Нажать кнопку «Создать», ввести имя для новой роли (рис. 215) и нажать клавишу «Enter» на клавиатуре.
3. Выбрать необходимые привилегии для роли и нажать кнопку «Сохранить» в блоке «Действия».
4. Открыть вкладку «Состояние» и нажать кнопку «Синхронизировать» или выбрать соответствующий пункт из контекстного меню (подробнее см. п. 3.5 «Синхронизация»).

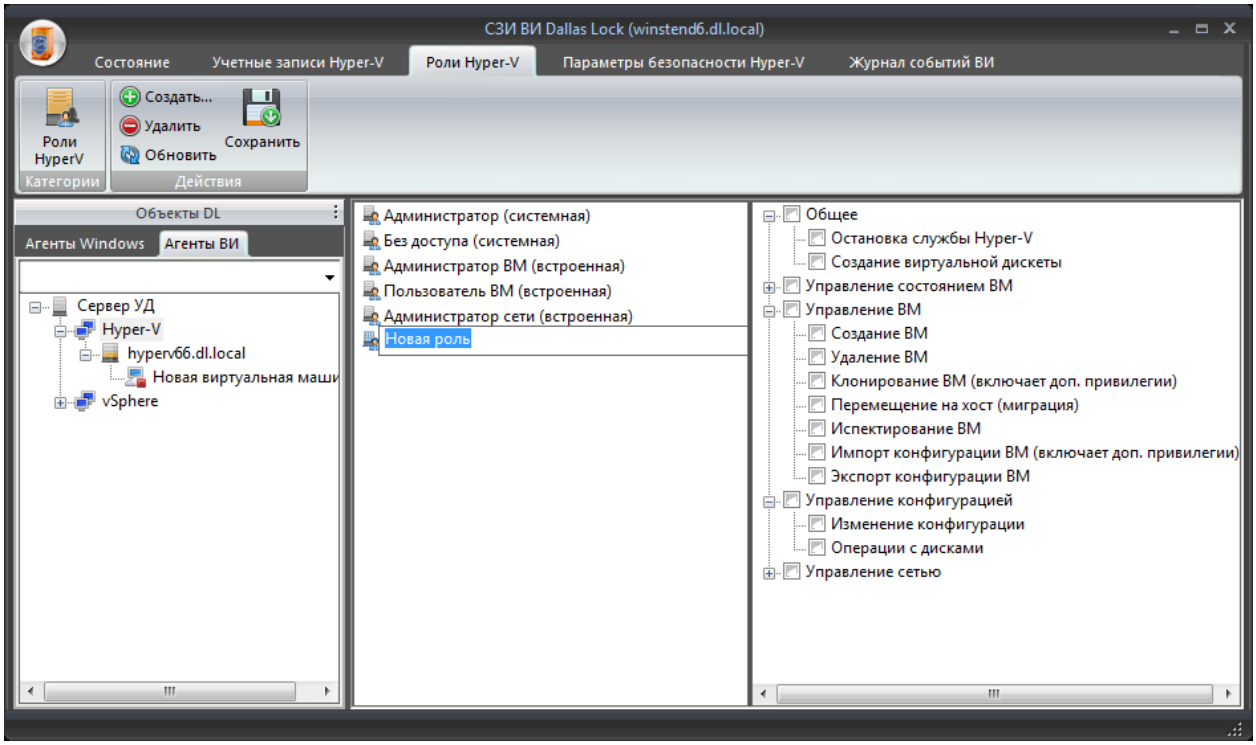


Рис. 215 – Создание роли Hyper-V

Все роли, за исключением системных ролей, можно переименовывать.

По умолчанию все привилегии для вновь созданных ролей отключены. Для назначения привилегий, необходимо корректно заполнить поле с привилегиями и нажать кнопку «Сохранить» в блоке «Действия».

После внесения всех необходимых изменений, следует выполнить сохранение путем нажатия кнопки «Сохранить» в блоке «Действия». Изменения будут применены после синхронизации (подробнее см. п. 3.5 «Синхронизация»).

6.4.2.2 Удаление ролей Hyper-V

Для удаления роли необходимо выделить роль, которую следует удалить и нажать кнопку «Удалить». При этом на экране появится предупреждение (рис. 216).

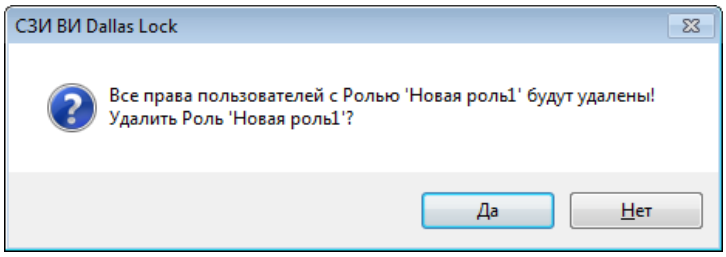


Рис. 216 – Удаление роли Hyper-V

После чего подтвердить операцию. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

После удаления назначенной роли все назначения данной роли удаляются.

Для обновления списка ролей в категории «Действия» необходимо нажать кнопку «Обновить».

6.4.3 Ролевая модель учетных записей KVM

Настройки по правам администрирования доступа к гипервизорам, объектам ВИ и виртуальным машинам KVM осуществляются средствами ролевой модели разграничения доступа. Для просмотра и редактирования параметров ролевого доступа необходимо в дереве «Агенты ВИ» на уровне группы KVM перейти на вкладку «Роли KVM» (рис. 217).

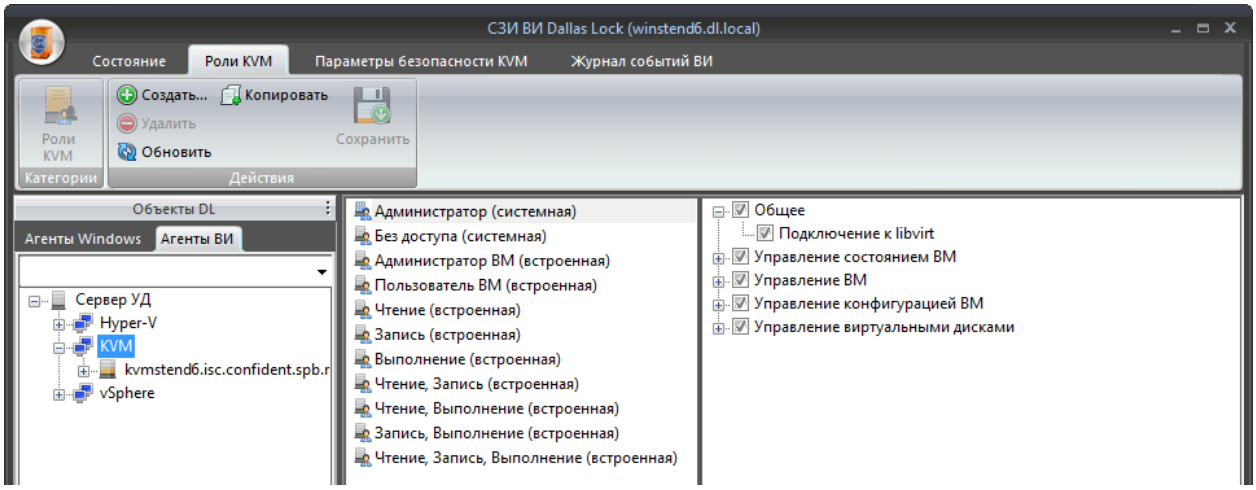


Рис. 217 – Роли KVM

В группе KVM на вкладке «Роли KVM» присутствуют предустановленные роли, которые невозможно изменить (системные). Системные предустановленные роли, которые нельзя изменить или удалить, называются (Администратор и Без доступа).

Для системных ролей установлены следующие разрешающие привилегии:

- для роли «Администратор»: включены все привилегии;
- для роли «Без доступа»: все привилегии отключены.

Предустановленные роли, привилегии которых можно редактировать:

- Администратор ВМ;
- Пользователь ВМ;
- Чтение;
- Запись;
- Выполнение;
- Чтение, Запись;
- Чтение, Выполнение;
- Запись, Выполнение;
- Чтение, Запись, Выполнение.

Также, следует учитывать, что редактирование ролей осуществляется на общем для всех СВ KVM уровне, следовательно, на каждом СВ KVM всегда создается одинаковый набор ролей.

6.4.3.1 Создание ролей KVM

Для создания новой роли необходимо:

1. Выбрать уровень группы KVM и открыть вкладку «Роли KVM».

2. Нажать кнопку «Создать», ввести имя для новой роли (рис. 218) и нажать клавишу «Enter» на клавиатуре.

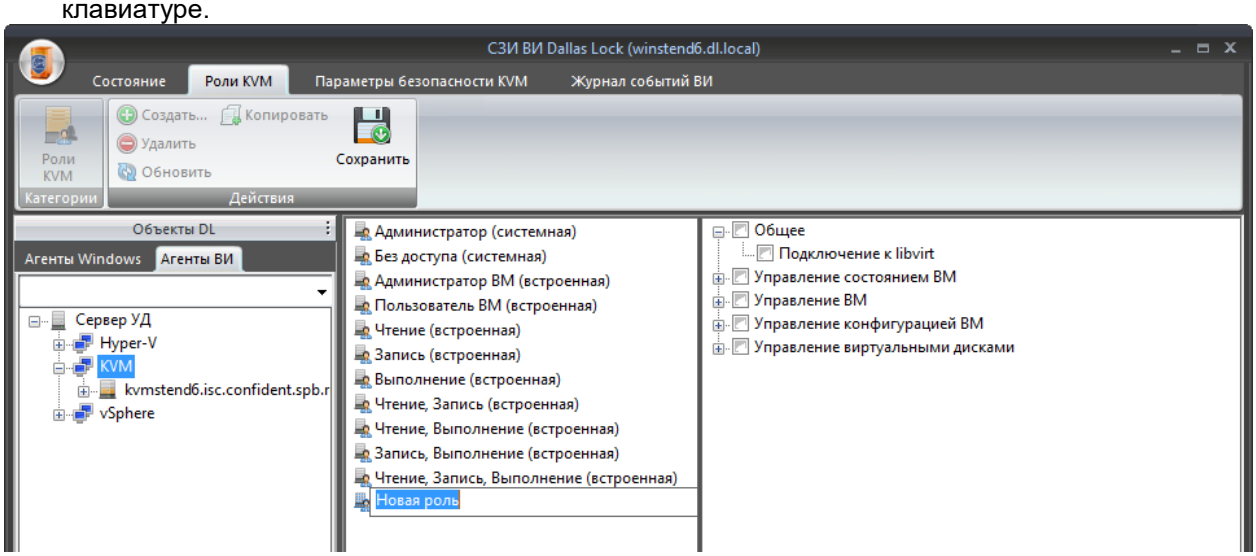


Рис. 218 – Создание роли KVM

3. Выбрать необходимые привилегии для роли и нажать кнопку «Сохранить» в блоке «Действия».
4. Открыть вкладку «Состояние» и нажать кнопку «Синхронизировать» или выбрать соответствующий пункт из контекстного меню (подробнее см. п. 3.5 «Синхронизация»).

Все роли, за исключением системных ролей, можно переименовывать.

По умолчанию все привилегии для вновь созданных ролей отключены. Для назначения привилегий, необходимо корректно заполнить поле с привилегиями и нажать кнопку «Сохранить» в блоке «Действия».

После внесения всех необходимых изменений, следует выполнить сохранение путем нажатия кнопки «Сохранить» в блоке «Действия». Изменения будут применены после синхронизации (подробнее см. п. 3.5 «Синхронизация»).

6.4.3.2 Удаление ролей KVM

Для удаления роли необходимо выделить роль, которую следует удалить и нажать кнопку «Удалить». При этом на экране появится предупреждение (рис. 219).

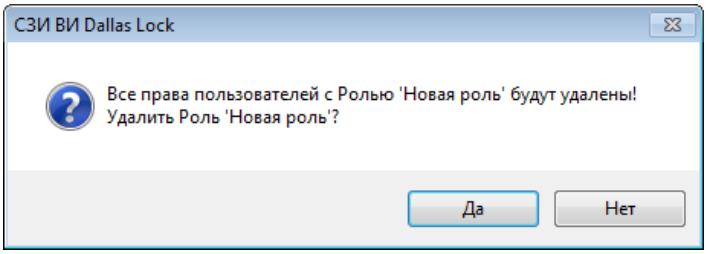


Рис. 219 – Удаление роли KVM

После чего подтвердить операцию. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

После удаления назначенной роли все назначения данной роли удаляются.

Для обновления списка ролей в категории «Действия» необходимо нажать кнопку «Обновить».

6.4.4 Ролевая модель учетных записей oVirt/zVirt/HOSTVM/РЕД Вирт

Настройки по правам администрирования доступа к гипервизорам, объектам ВИ и виртуальным машинам oVirt/zVirt/HOSTVM/РЕД Вирт осуществляются средствами ролевой модели разграничения доступа. Для просмотра и редактирования параметров ролевого доступа необходимо в дереве «Агенты ВИ» на уровне СВ oVirt/zVirt/HOSTVM/РЕД Вирт перейти на вкладку «Роли oVirt/zVirt/HOSTVM/РЕД Вирт» (рис. 220).

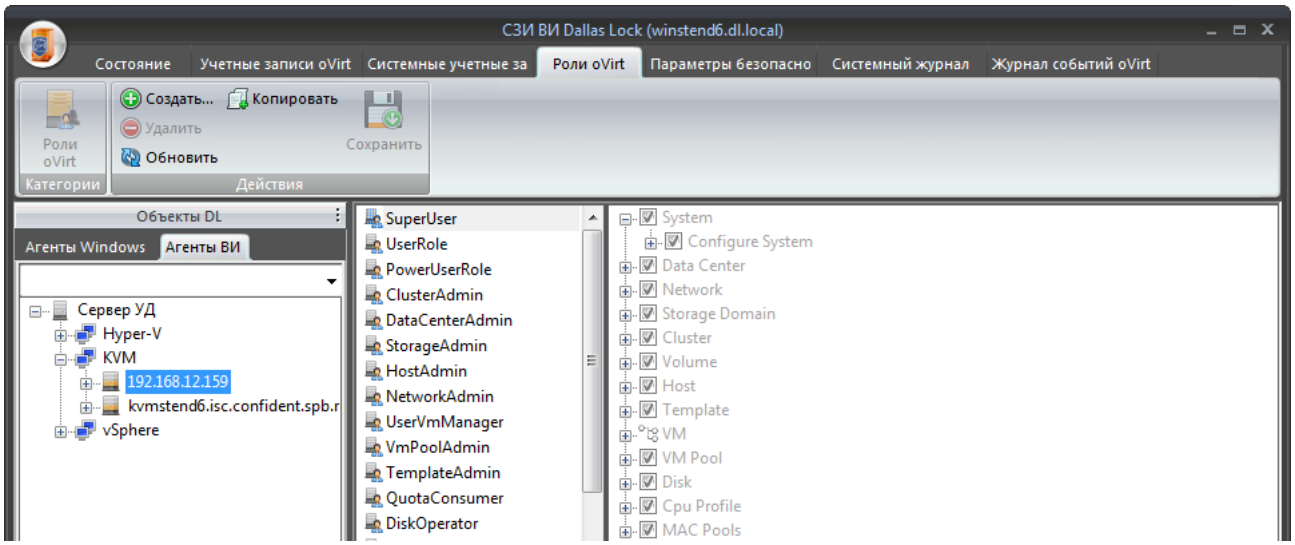


Рис. 220 – Роли oVirt/zVirt/HOSTVM/РЕД Вирт

На уровне СВ oVirt/zVirt/HOSTVM/РЕД Вирт на вкладке «Роли oVirt/zVirt/HOSTVM/РЕД Вирт» присутствуют предустановленные роли, которые невозможно изменить (системные), предустановленные роли, привилегии которых можно редактировать, а также существует возможность создания новых ролей.

Системные предустановленные роли, которые нельзя изменить или удалить, полностью соответствуют стандартным предустановленным ролям oVirt/zVirt/HOSTVM/РЕД Вирт.

Предустановленные роли СЗИ ВИ, которые нельзя изменить или удалить:

- Read;
- Write;
- Execute;
- Read - Write;
- Read - Execute;
- Write - Execute;
- Read – Write - Execute.

6.4.4.1 Создание ролей oVirt/zVirt/HOSTVM/РЕД Вирт

Для создания новой роли необходимо:

1. Выбрать уровень СВ oVirt/zVirt/HOSTVM/РЕД Вирт и открыть вкладку «Роли oVirt/zVirt/HOSTVM/РЕД Вирт».
2. Нажать кнопку «Создать», ввести имя для новой роли (рис. 221) и нажать клавишу «Enter» на клавиатуре.

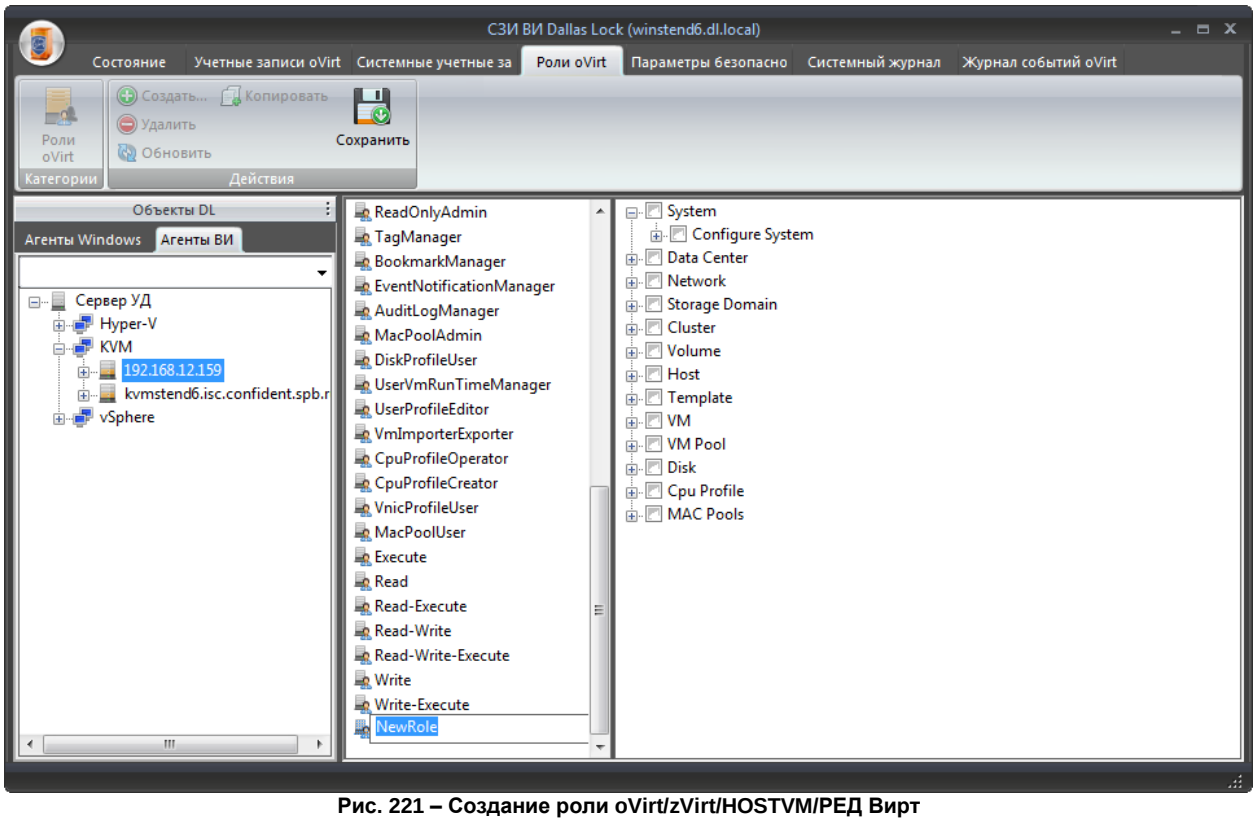


Рис. 221 – Создание роли oVirt/zVirt/HOSTVM/РЕД Вирт

3. Выбрать необходимые привилегии для роли и нажать кнопку «Сохранить» в блоке «Действия».
4. Открыть вкладку «Состояние» и нажать кнопку «Синхронизировать» или выбрать соответствующий пункт из контекстного меню (подробнее см. п. 3.5 «Синхронизация»).

Все роли, за исключением системных и предустановленных ролей, можно переименовывать.

По умолчанию все привилегии для вновь созданных ролей отключены. Для назначения привилегий, необходимо корректно заполнить поле с привилегиями и нажать кнопку «Сохранить» в блоке «Действия».

После внесения всех необходимых изменений, следует выполнить сохранение путем нажатия кнопки «Сохранить» в блоке «Действия». Изменения будут применены после синхронизации (подробнее см. п. 3.5 «Синхронизация»).

6.4.4.2 Удаление ролей oVirt/zVirt/HOSTVM/РЕД Вирт

Для удаления роли необходимо выделить роль, которую следует удалить и нажать кнопку «Удалить». При этом на экране появится предупреждение (рис. 222).

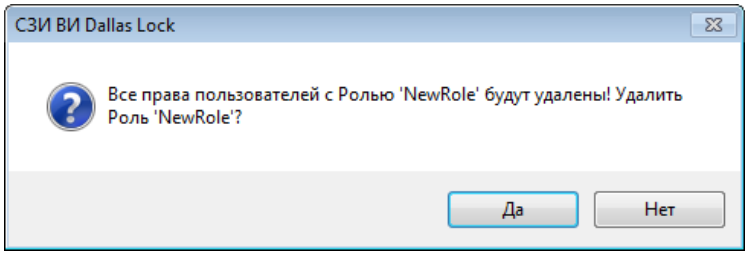


Рис. 222 – Удаление роли oVirt/zVirt/HOSTVM/РЕД Вирт

После чего подтвердить операцию. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

После удаления назначенной роли все назначения данной роли удаляются.

Для обновления списка ролей в категории «Действия» необходимо нажать кнопку «Обновить».

6.4.5 Права пользователей

Назначение ролей может осуществляться на уровне СВ, датацентра, кластера, гипервизора или ВМ, при этом настройки СВ могут наследоваться датацентром, кластером, гипервизором, ВМ (подробнее см. п. 3.8 «Наследование настроек»).

Просмотр и редактирование прав пользователей для vSphere происходит на уровне Сервера виртуализации в категории «Параметры безопасности vSphere» → «Права пользователей» (рис. 223).

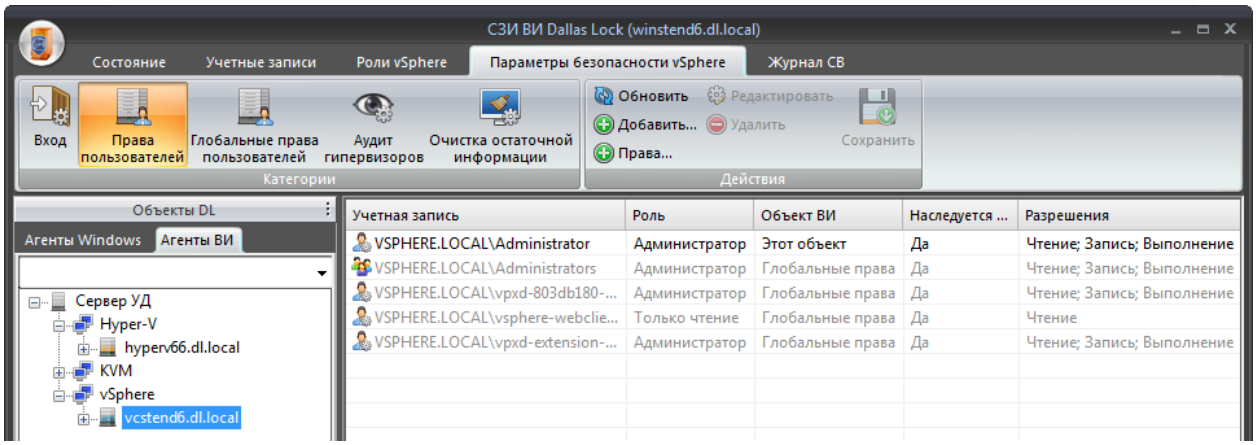


Рис. 223 – Права пользователей vSphere

Просмотр и редактирование прав пользователей для Hyper-V происходит на уровне Сервера виртуализации в категории «Параметры безопасности Hyper-V» → «Права пользователей» (рис. 224).

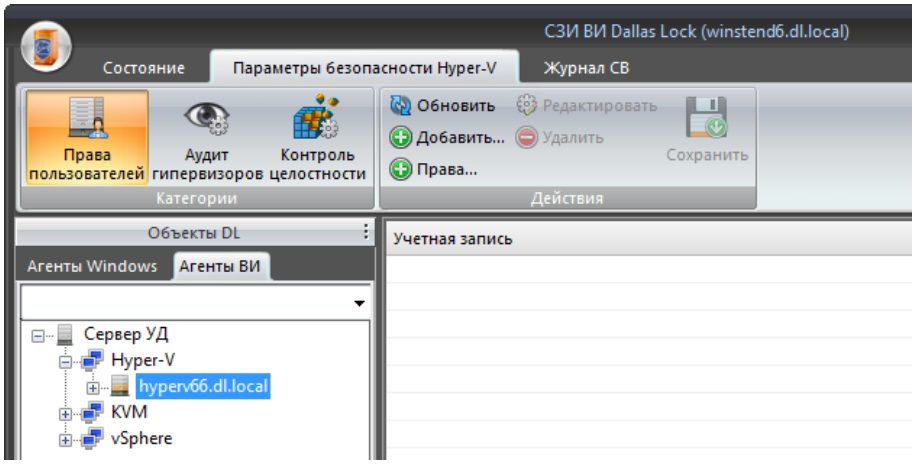


Рис. 224 – Права пользователей Hyper-V

Просмотр и редактирование прав пользователей для KVM происходит на уровне Сервера виртуализации в категории «Параметры безопасности KVM» → «Права пользователей» (рис. 225).

Примечание. Для предоставления доступа новому пользователю к управлению ВМ необходимо добавить данного пользователя в следующие группы:

1. Для ОС Linux Mint – libvirt.
2. Для ОС Ubuntu – libvirt, kvm.
3. Для ОС Astra Linux (Орел 2.12) – kvm, libvirt, libvirt-qemu.
4. Для ОС Astra Linux (Смоленск 1.6) – kvm, libvirt, libvirt-qemu, libvirt-admin.
5. Для ОС CentOS – kvm.

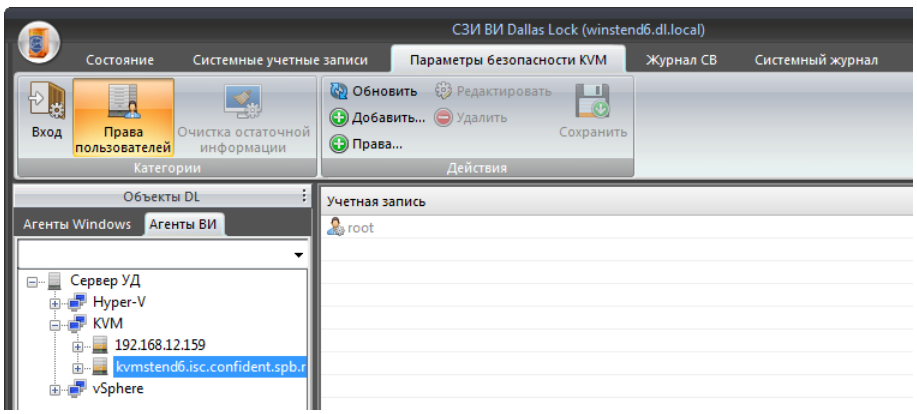


Рис. 225 – Права пользователей KVM

Просмотр и редактирование прав пользователей для oVirt/zVirt/HOSTVM/РЕД Вирт происходит на уровне Сервера виртуализации в категории «Параметры безопасности KVM» → «Права

пользователей» (рис. 226).

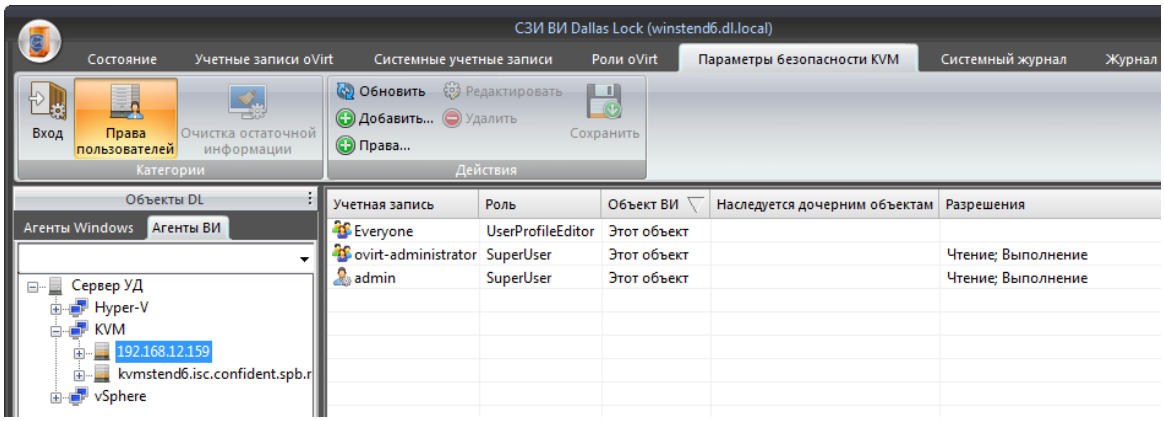


Рис. 226 – Права пользователей oVirt/zVirt/HOSTVM/РЕД Вирт

Для пользователя или группы может быть назначена только одна роль на объект, однако, привилегии для пользователя могут суммироваться, если он состоит в нескольких группах, для которых назначены разные роли на объект.

Исключением является случай, когда роль явно назначается пользователю. В таком случае она перекрывает все привилегии, полученные от групп.

Чтобы задать пользователю или группе определенную роль необходимо:

1. Выбрать уровень Сервера виртуализации и открыть категорию «Параметры безопасности СВ» → «Права пользователей».
2. Нажать кнопку «Добавить», после чего появится окно со списком пользователей и групп, которым будет задана роль (рис. 227).

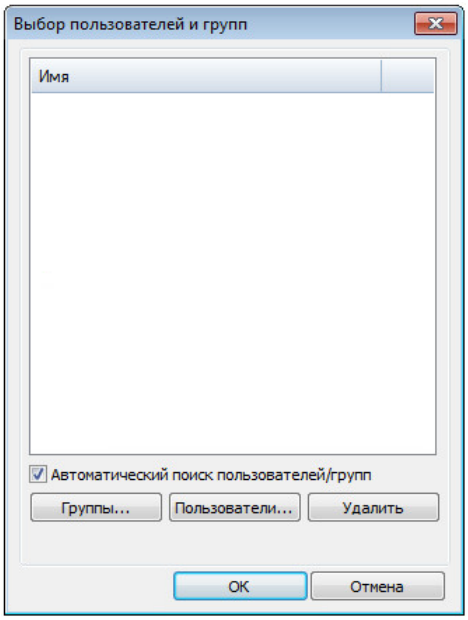


Рис. 227 – Выбор пользователей и групп

3. Отметив пункт «Автоматический поиск пользователей/групп» при последующем нажатии кнопок «Пользователи» или «Группы» будет показан список всех возможных пользователей или групп для последующего назначения роли.

Примечание. При добавлении прав пользователя для локального пользователя Windows данный пользователь должен быть синхронизирован на Сервере виртуализации (vCenter).

4. Далее требуется выбрать пользователей и группы, которым будет задана роль, после чего нажать «ОК» (рис. 228).

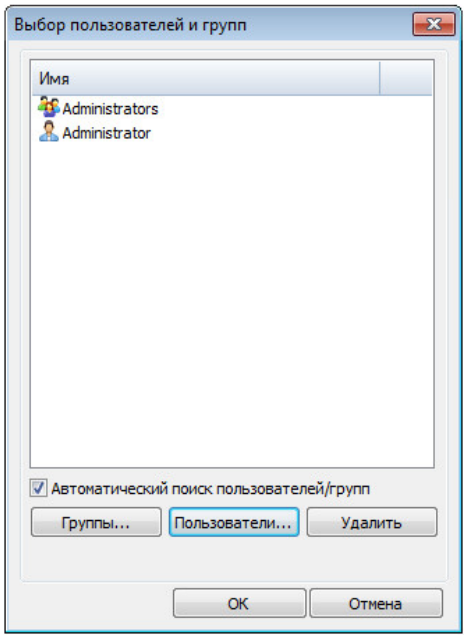


Рис. 228 – Выбор пользователей и групп

5. В появившемся окне выбрать роль из выпадающего списка (рис. 229).

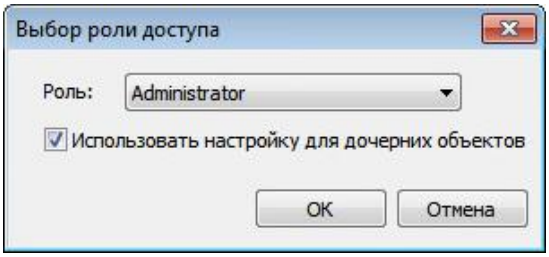


Рис. 229 – Выбор роли доступа

6. Чтобы распространить привилегии на дочерние объекты, необходимо установить флаг «Настройка действует на дочерние объекты».

Примечание. При назначении роли для KVM рекомендуется всегда устанавливать данный флаг.

7. Нажать кнопку «ОК».
8. Сохранить изменения, нажав кнопку «Сохранить».
9. Открыть вкладку «Состояние» и нажать кнопку «Синхронизировать».

Для редактирования прав пользователей необходимо:

1. Выделить нужную учетную запись или группу и выбрать действие «Редактировать»,
2. В появившемся окне выбрать роль из выпадающего списка.
3. Чтобы распространить привилегии на дочерние объекты, необходимо установить флаг «Настройка действует на дочерние объекты».
4. Нажать кнопку «ОК».
5. Сохранить изменения, нажав кнопку «Сохранить».
6. Открыть вкладку «Состояние» и нажать кнопку «Синхронизировать».

Для удаления прав пользователей необходимо выбрать учетную запись или группу и нажать кнопку «Удалить». После чего подтвердить операцию, сохранить изменения и синхронизировать.

Для обновления списка учетных записей в категории «Действия» необходимо нажать кнопку «Обновить».

6.4.5.1 Глобальные права пользователей vSphere

Глобальные права доступа пользователей имеют наивысший приоритет и автоматически наследуются на дочерние объекты ВИ. Порядок настройки глобальных прав для СВ vCenter и vCSA идентичен.

Внимание! Осуществлять настройку глобальных прав пользователей может только суперадминистратор.

Для просмотра, добавления, удаления и редакции глобальных прав доступа пользователей необходимо на уровне Сервера виртуализации перейти к категории «Параметры безопасности vSphere» → «Глобальные права пользователей» (рис. 230).

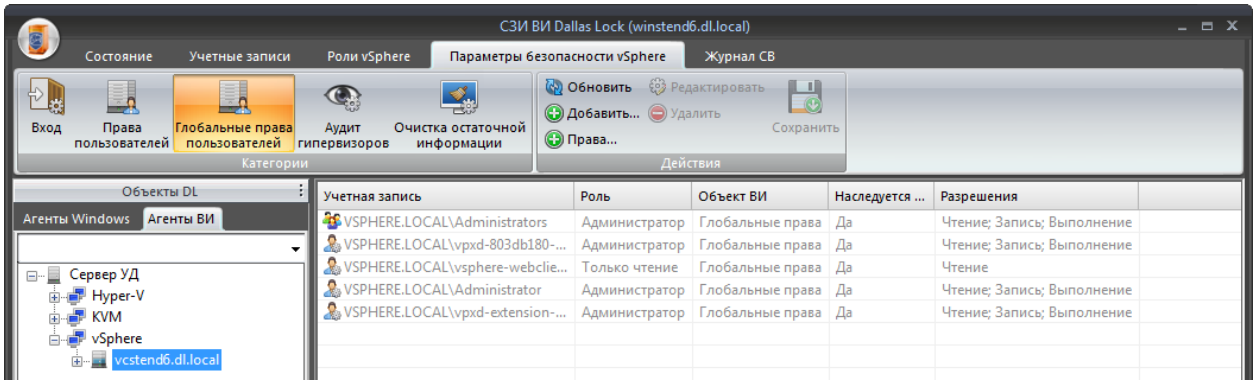


Рис. 230 – Глобальные права доступа пользователей vSphere

Глобальные права можно назначить пользователю либо группе пользователей. Для этого необходимо:

1. В категории «Действия» нажать кнопку «Добавить».
2. В появившемся окне нажать кнопку «Группы» либо «Пользователи».
3. Выбрать одну или несколько групп или пользователей (рис. 231), нажать кнопку «ОК».

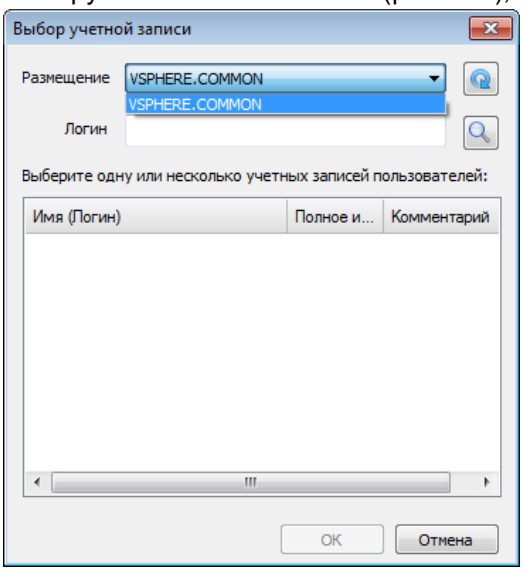


Рис. 231 – Добавление учетных записей

4. Нажать кнопку «ОК», а затем в категории действий кнопку «Сохранить».

Для изменения роли учетной записи и наследования настройки для дочерних объектов, необходимо выбрать учетную запись и в категории «Действия», либо в контекстном меню, вызываемом нажатием правой кнопкой мыши на учетной записи, нажать кнопку «Редактировать». В появившемся окне выбрать необходимые параметры, нажать кнопку «ОК». Затем нажать кнопку «Сохранить», чтобы изменения вступили в силу.

Для удаления учетной записи, которой назначены глобальные права, необходимо выбрать учетную запись и, либо в категории «Действия», либо в контекстном меню, вызываемом нажатием правой кнопкой мыши на учетной записи, нажать кнопку «Удалить».

Просмотр, добавление, удаление и редактирование учетных записей, наделенных глобальными правами на уровнях дата центра, кластера гипервизоров, виртуальных машин и гипервизоров, производится на вкладках «Параметры безопасности» → «Права пользователей».

Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

6.4.5.2 Назначение прав пользователям vSphere

1. Для назначения разрешений пользователю, на уровне СВ следует перейти на вкладку «Параметры безопасности vSphere», выбрать категорию «Права пользователей», во вкладке действия нажать кнопку «Добавить» (рис. 232).

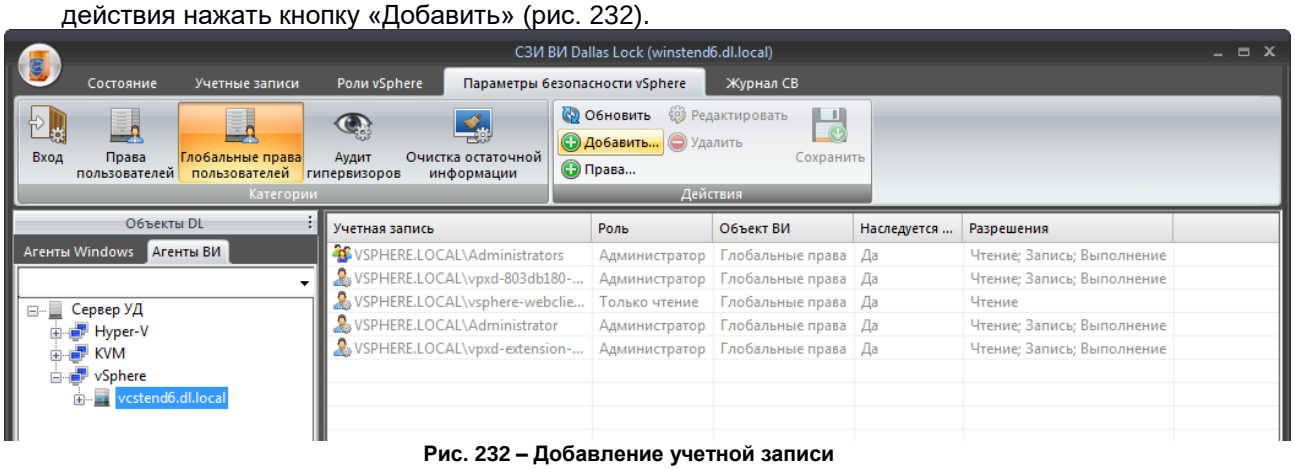


Рис. 232 – Добавление учетной записи

2. В появившемся окне нажать кнопку «Группы» либо «Пользователи».
3. Выбрать размещение группы или пользователя из выпадающего меню (рис. 233), после чего выбрать из списка одну или несколько групп или пользователей и нажать кнопку «ОК» в обеих окнах.

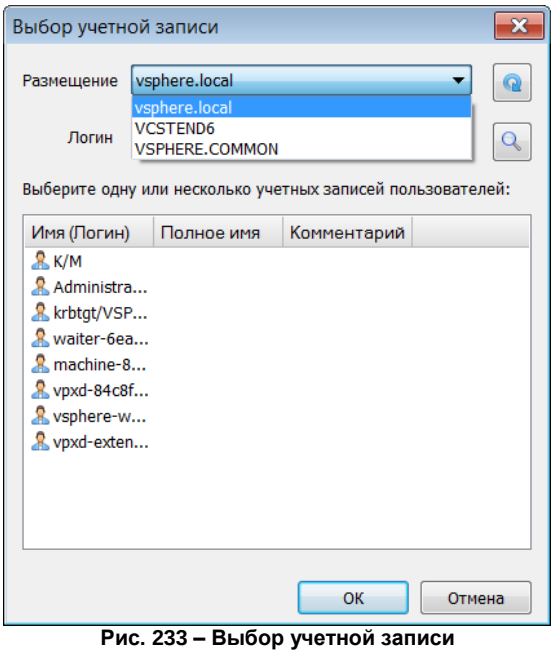


Рис. 233 – Выбор учетной записи

4. В появившемся окне выбрать роль для учетной записи из выпадающего списка и нажать на кнопку «ОК».
5. Далее необходимо в блоке «Действия» нажать кнопку «Сохранить».
6. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

6.4.5.3 Назначение прав пользователям гипервизора ESXi

Назначение прав пользователям гипервизора осуществляется на уровне гипервизора во вкладке «Параметры безопасности vSphere».

Назначение прав локальным пользователям гипервизора ESXi

Перед назначением прав пользователям, необходимо убедиться, что данные учетные записи активированы (подробнее см. п. 5.1.4 «Активация и деактивация учетных записей»).

1. Для назначения разрешений локальному пользователю гипервизора, следует выбрать категорию «Права пользователей гипервизоров», в блоке «Действия» нажать кнопку «Добавить».
2. В появившемся окне необходимо нажать кнопку «Пользователи», после чего выбрать из списка учетную запись и нажать кнопку «ОК» в обеих окнах (рис. 234).

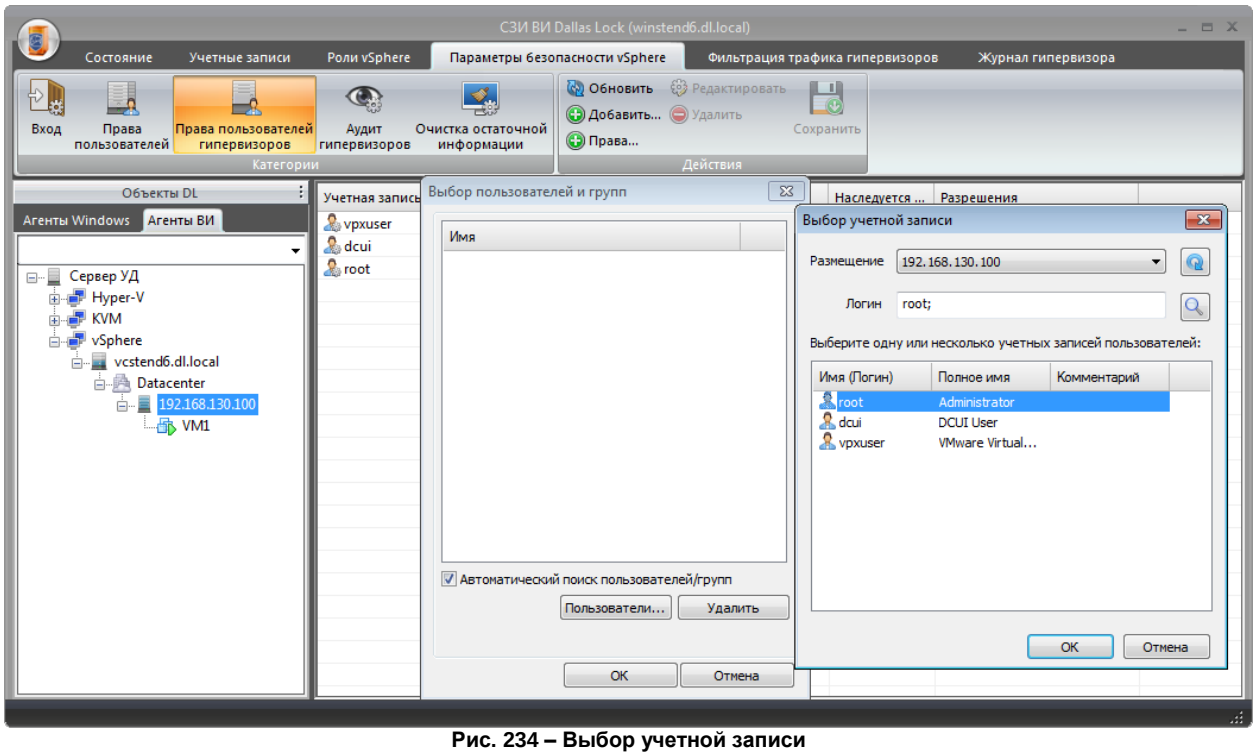


Рис. 234 – Выбор учетной записи

3. В появившемся окне выбрать роль из выпадающего меню для учетной записи из выпадающего списка (рис. 235) и нажать на кнопку «ОК».

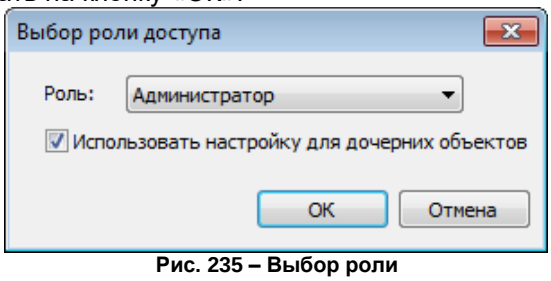


Рис. 235 – Выбор роли

4. Далее необходимо в блоке «Действия» нажать кнопку «Сохранить».

5. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

Назначение прав доменным пользователям гипервизора ESXi

1. Для назначения разрешений доменным пользователям или группам, следует выбрать категорию «Права пользователей», в блоке «Действия» нажать кнопку «Добавить».

2. В появившемся окне необходимо нажать кнопку «Группы» или «Пользователи», после чего выбрать из выпадающего меню размещение групп или пользователей. Далее из списка выбрать одну или несколько групп или пользователей и нажать кнопку «ОК» в обеих окнах (рис. 236).

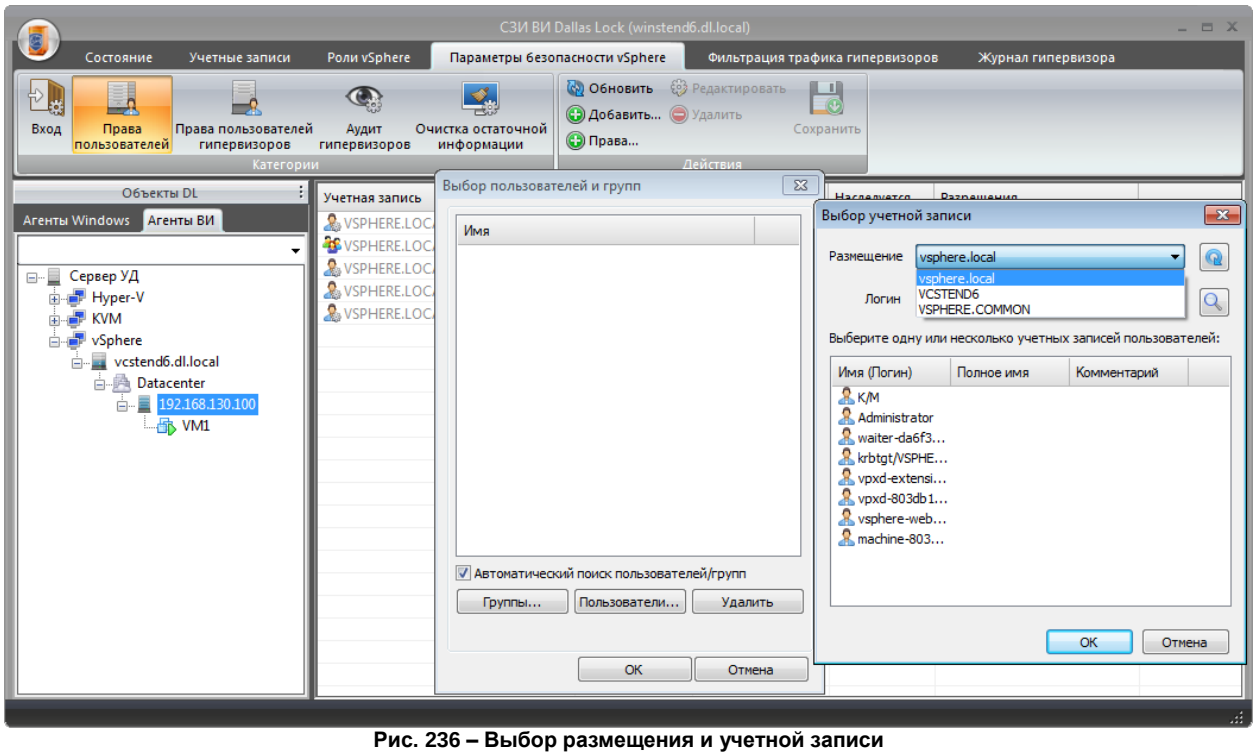


Рис. 236 – Выбор размещения и учетной записи

3. В появившемся окне выбрать роль из выпадающего меню для учетной записи из выпадающего списка и нажать на кнопку «ОК». Чтобы распространить привилегии на дочерние объекты, необходимо установить флаг «Использовать настройку для дочерних объектов».

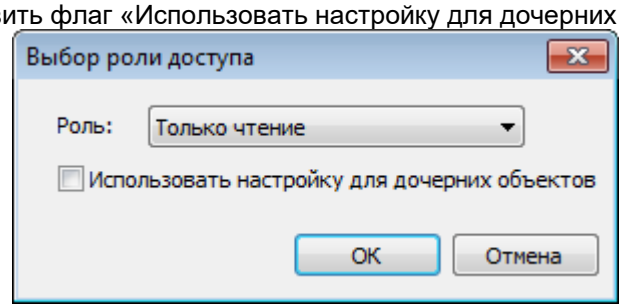


Рис. 237 – Выбор роли

4. Далее необходимо в блоке «Действия» нажать кнопку «Сохранить».

5. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

6.4.5.4 Упрощенное назначение прав доступа пользователям

Данная опция позволяет назначать права доступа пользователям к объектам ВИ по средствам выбора типа действия с объектом ВИ.

Доступны следующие типы действий:

- Чтение.
- Запись.
- Выполнение.

Для назначения прав доступа необходимо:

1. Выбрать уровень СВ, гипервизора или ВМ и открыть категорию «Параметры безопасности» → «Права пользователей», в блоке «Действия» нажать кнопку «Права» (рис. 238).

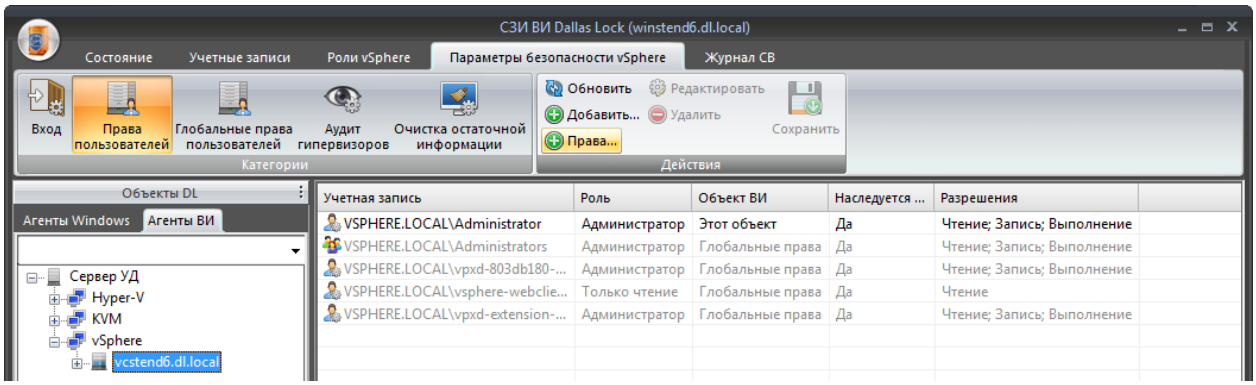


Рис. 238 – Упрощенное назначение прав

2. В появившемся окне нажать кнопку «Группы» либо «Пользователи».

Отметив пункт «Автоматический поиск пользователей/групп» при последующем нажатии кнопок «Пользователи» или «Группы» будет показан список всех возможных пользователей или групп для последующего назначения роли.

Примечание. При добавлении прав пользователя для локального пользователя Windows данный пользователь должен быть синхронизирован на Сервере виртуализации (vCenter).

3. Выбрать размещение группы или пользователя из выпадающего меню (рис. 239), после чего выбрать из списка одну или несколько групп, или пользователей и нажать кнопку «ОК» в обеих окнах.

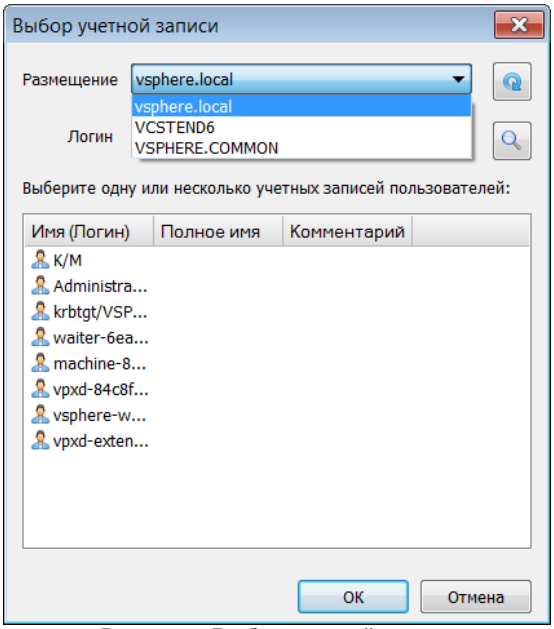


Рис. 239 – Выбор учетной записи

4. В появившемся окне выбрать разрешенные действия, для назначения соответствующей роли и нажать на кнопку «ОК» (рис. 240). Чтобы распространить привилегии на дочерние объекты, необходимо установить флаг «Использовать настройку для дочерних объектов».

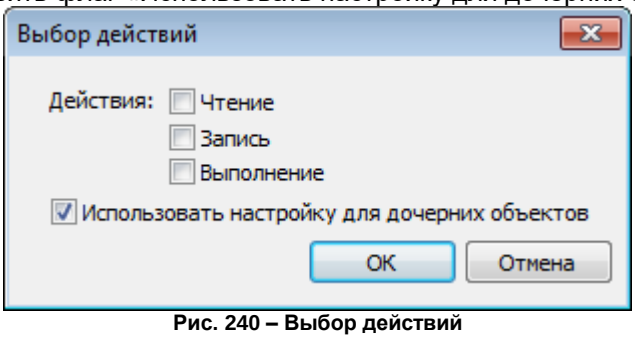


Рис. 240 – Выбор действий

5. Сохранить изменения, нажав кнопку «Сохранить».

6. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

6.5 Настройка фильтрации трафика гипервизоров ESXi

Гипервизор ESXi включает в себя брандмауэр между интерфейсом управления и сетью. По умолчанию брандмауэр гипервизора настроен на блокирование входящего и исходящего трафика, за исключением трафика для его стандартных служб. Первоначально подключение к данным службам доступно всем.

Просмотр и редактирование списка правил фильтрации трафика для всех гипервизоров происходит на уровне «vSphere» на вкладке «Фильтрация трафика гипервизоров» (рис. 241).

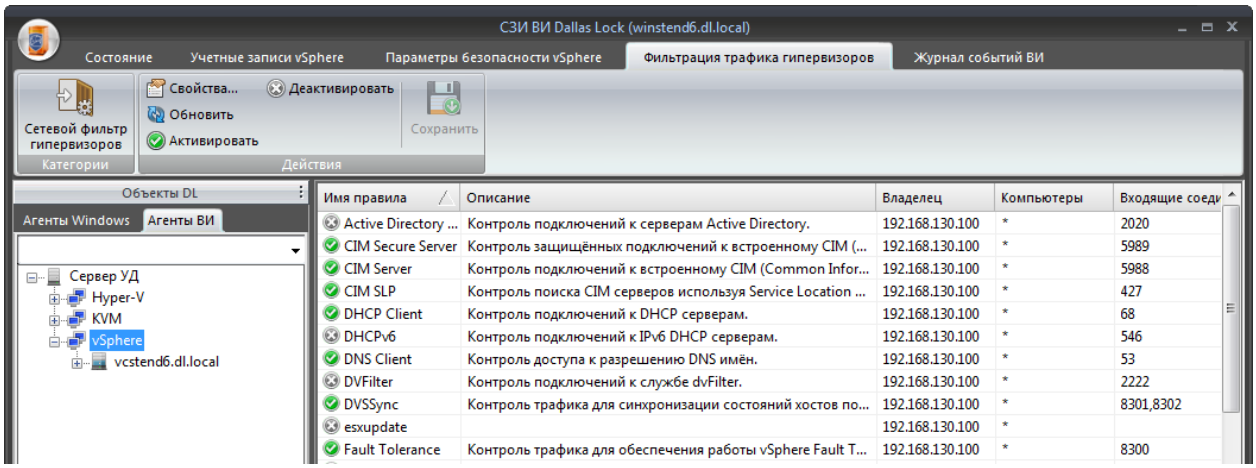


Рис. 241 – Фильтрация трафика гипервизора

После установки агента DL ESXi (добавления гипервизора в ВИ DL) выполняется вычитывание списка правил фильтрации гипервизора. Далее эти правила пополняют общий список правил ЦУ СЗИ ВИ на уровне «vSphere» на вкладке «Фильтрация трафика гипервизоров». В общий список правил добавляются только новые правила с оригинальным именем. Список общих правил ЦУ СЗИ ВИ возможно наследовать на все гипервизоры ВИ.

Если при вычитывании правил, имя правила гипервизора совпадает с именем правила из общего списка, но имеет другое значение (порт, IP-адрес и т.д.), то данное правило не добавляется в общий список и отмечается на уровне добавленного гипервизора как оригинальное (т.е. не наследуется).

Если при вычитывании правил, имя правила гипервизора совпадает с именем правила из общего списка и имеет такое же значение, то данное правило отмечается на уровне гипервизора как наследуемое (см. п. 3.8 «Наследование настроек»).

Редакция (переопределение) правил фильтрации доступно для каждого отдельного гипервизора. Для этого необходимо перейти на уровень гипервизора во вкладку «Фильтрация трафика гипервизора» (рис. 242). Здесь:

 — отмечанное флагом поле означает, что правило будет применено при синхронизации с гипервизором;

 — пустое поле означает, что изменение настройки правила при синхронизации с гипервизором применяться не будет.

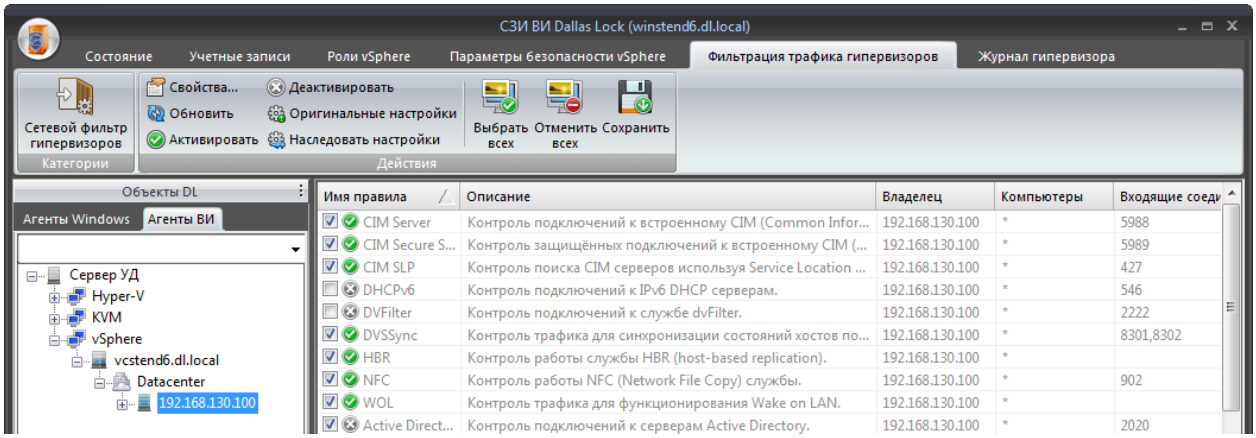


Рис. 242 – Переопределение правил фильтрации на гипервизоре

Вспомогательные кнопки помогают одновременно выбрать и отменить все правила.

Если при вычитывании правил гипервизора 1, имя правила гипервизора 1 не совпадает с именем из

общего списка, то данное правило добавляется в общий список. Также правило гипервизора 1 не отмечается флагом в списке правил на гипервизоре 2, где данного правила не было при вычитывании правил гипервизора 2.

После формирования списка правил необходимо нажать кнопку «Сохранить», после чего перейти на вкладку «Состояние» и нажать кнопку «Синхронизировать».

Примечание. Для работы с хранилищем данных NFS необходимо используя Консоль включить правило «NFS Client» (рис. 243).

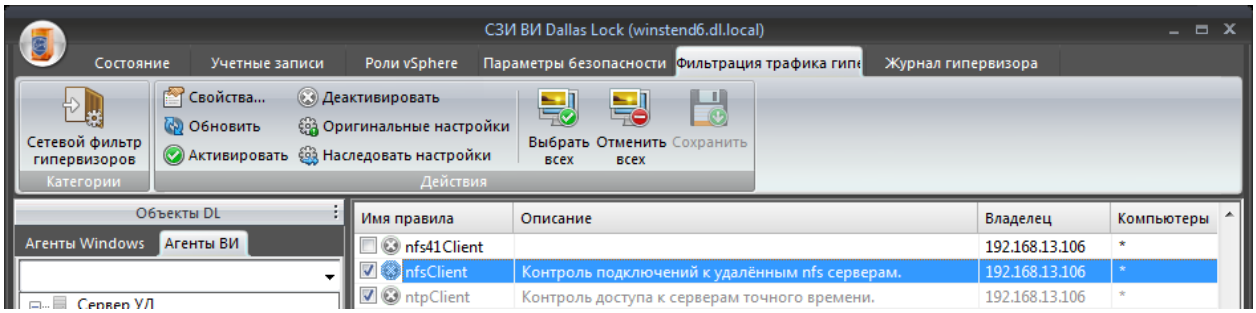


Рис. 243 – Правило «NFS Client»

Для редактирования правила фильтрации для всех гипервизоров ВИ, необходимо:

1. Выбрать уровень «vSphere» и открыть вкладку «Фильтрация трафика гипервизоров».
2. Выделить необходимую службу и нажать кнопку «Свойства».
3. В появившемся окне нажать кнопку «Добавить» (рис. 244).

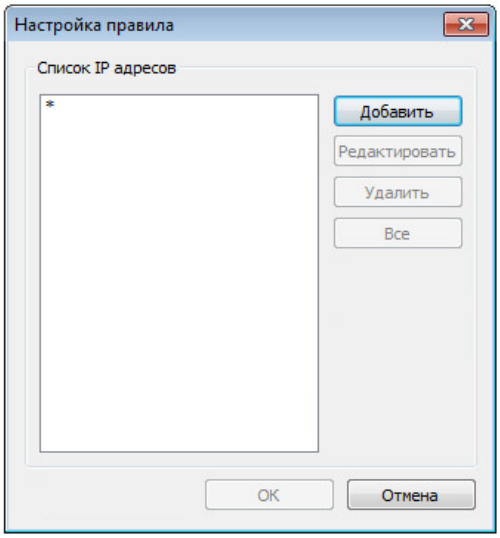


Рис. 244 – Настройка правила фильтрации трафика гипервизора

4. Далее откроется окно «Назначение IP-адреса», где нужно ввести доверенный IP-адрес или полное доменное имя. Также возможно задать диапазон IP-адресов, дополнительно установив флаг «Диапазон» и введя маску подсети (рис. 245). Нажать кнопку «ОК».

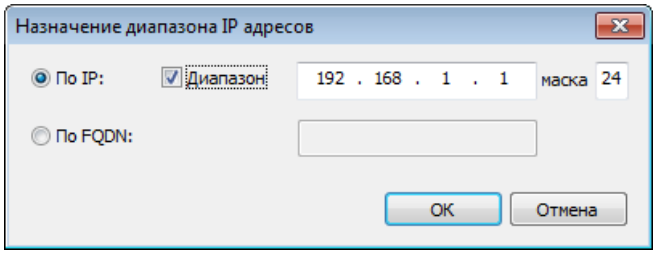


Рис. 245 – Назначение диапазона IP-адресов

5. Введенный IP-адрес отобразится в списке IP-адресов (рис. 246).

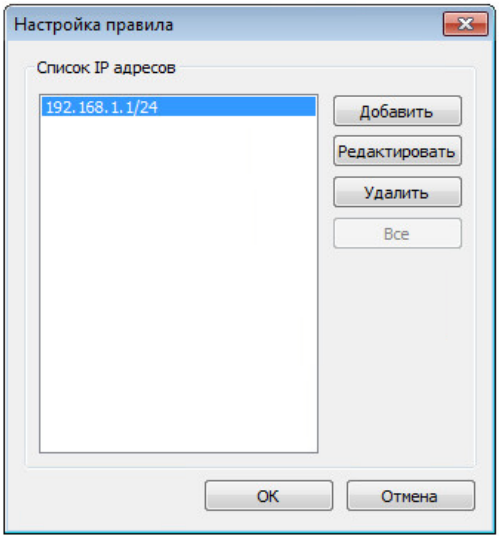


Рис. 246 – Настройка правила фильтрации трафика гипервизора

6. Чтобы отредактировать IP-адрес, необходимо выбрать его в списке IP-адресов и нажать кнопку «Редактировать».
7. Чтобы разрешить доступ всем, необходимо нажать кнопку «Все».
8. Чтобы удалить IP-адрес, необходимо выбрать его в «Списке IP-адресов» и нажать кнопку «Удалить».
9. По завершению редактирования списка доверенных IP-адресов, необходимо нажать кнопку «ОК».
10. Далее нажать кнопку «Сохранить».
11. Открыть вкладку «Состояние» и нажать кнопку «Синхронизировать».

6.6 Сегменты безопасности

СЗИ ВИ позволяет разделять виртуальные инфраструктуры vSphere[23] и Hyper-V на сегменты безопасности средствами VLAN.

Внимание! Для корректной работы с сегментами системному администратору необходимо предварительно настроить ВМ, которые будут добавлены в сегмент, в том числе и изолированный. У ВМ должны быть удалены все виртуальные адаптеры, т.к. при добавлении в сегмент виртуальный адаптер будет создан автоматически. Также системному администратору необходимо добавить ТС, с которого осуществляется доступ к сегментам или изолированной ВМ, в соответствующий VLAN.

Сегмент безопасности состоит из метки доступа, объектов и субъектов доступа.

В качестве объектов доступа, выделяемых в сегмент, выступают виртуальные машины (ВМ).

В качестве субъектов доступа к сегменту выступают следующие типы субъектов:

- локальные учетные записи/группы ОС Windows;
- учетные записи/группы, созданные средствами Active Directory.

6.6.1 Настройка сегментов безопасности

Просмотр и редактирование сегментов безопасности происходит в дереве «Агенты ВИ» на уровне «Сервер УД».

6.6.1.1 Создание сегмента безопасности

Для создания метки безопасности необходимо:

1. Открыть категорию «Состояние» → «Сегменты безопасности» (рис. 247).

[23] Только для vCenter for Windows.

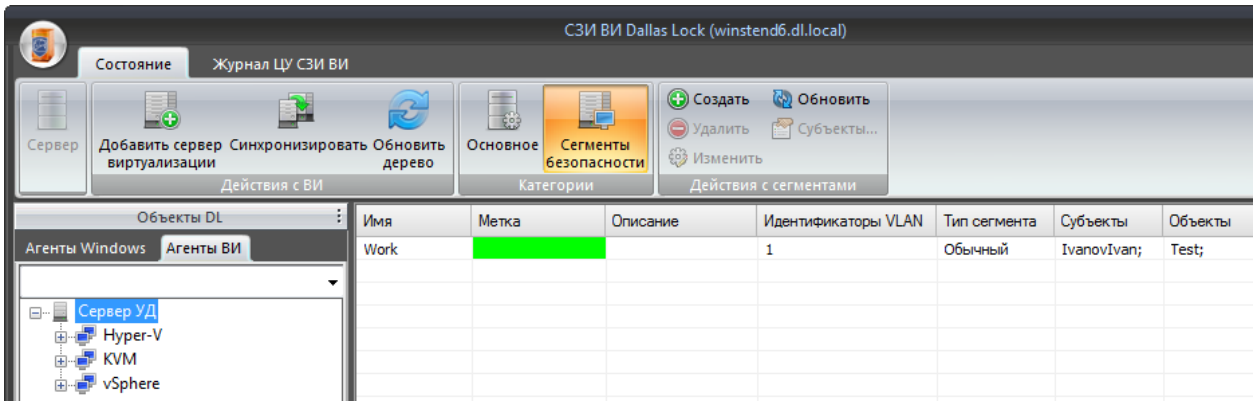


Рис. 247 – Сегменты безопасности

2. Нажать кнопку «Создать» в блоке «Действия с сегментами».
3. В появившемся окне (рис. 248) ввести имя сегмента, описание (опционально), если требуется, указать VLAN ID вручную, выбрать цвет метки (рис. 249), после чего нажать кнопку «ОК».

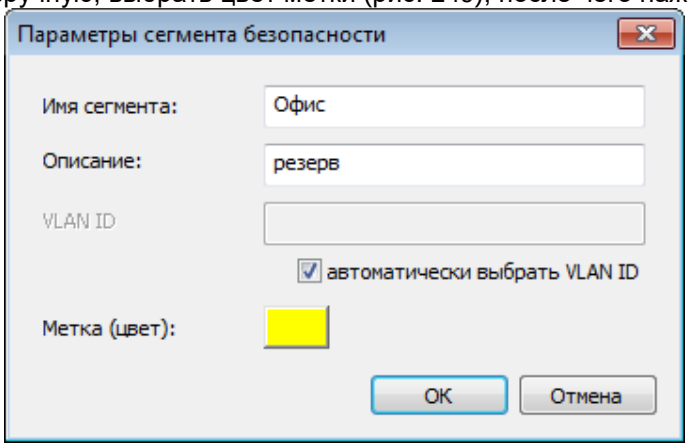


Рис. 248 – Создание сегмента безопасности

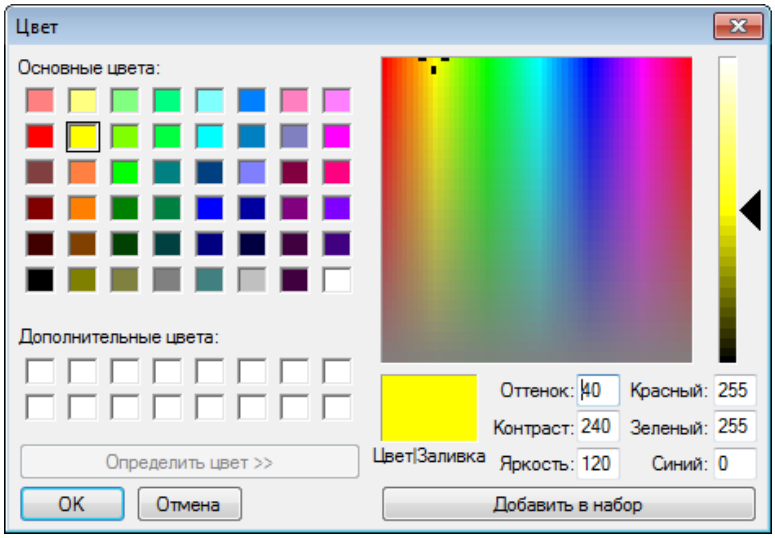


Рис. 249 – Выбор цвета метки

4. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

6.6.1.2 Редактирование списка учетных записей или групп в сегменте безопасности

Для редактирования списка учетных записей или групп в сегменте безопасности необходимо:

1. Открыть категорию «Состояние» → «Сегменты безопасности».
2. Выбрать сегмент из списка и нажать кнопку «Субъекты» (рис. 250).

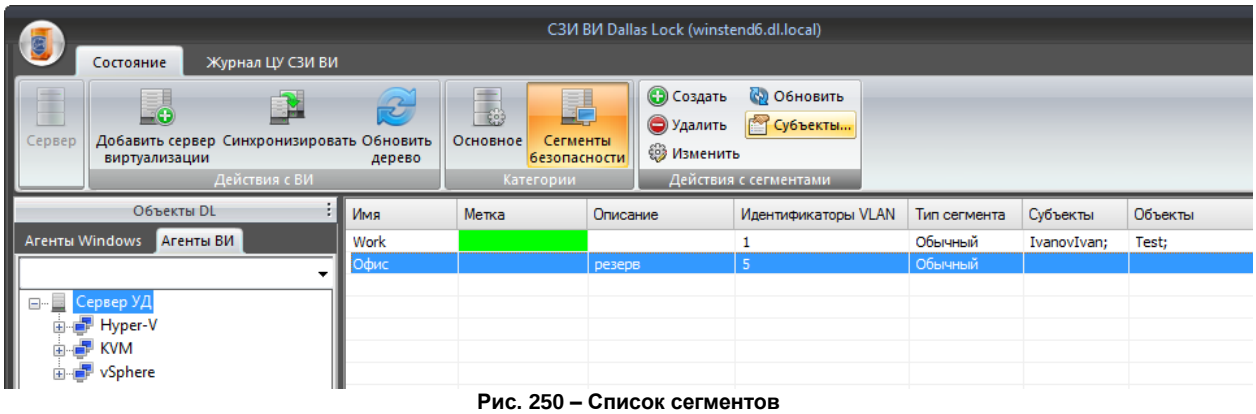


Рис. 250 – Список сегментов

3. В появившемся окне необходимо выбрать учетные записи или группы, которым будет предоставлен доступ к объектам ВИ в сегменте безопасности. При необходимости выбрать другой домен в выпадающем списке параметра «Список субъектов в домене» (рис. 251).

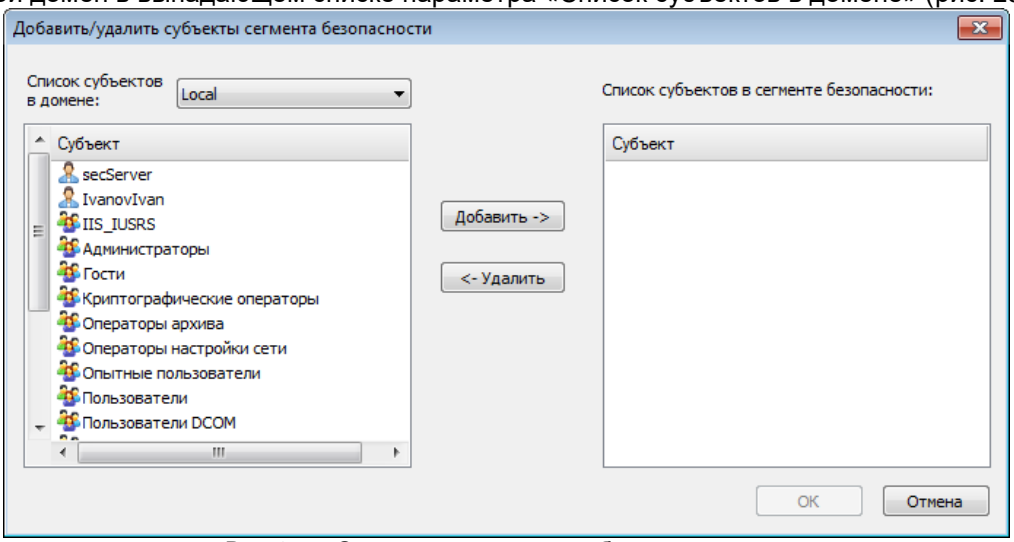


Рис. 251 – Окно редактирования субъектов сегмента

4. Выделить субъект в левом списке «Список субъектов в домене» и нажать кнопку «Добавить», после чего данный субъект будет перемещен в правый список «Список субъектов в группе» (рис. 252).

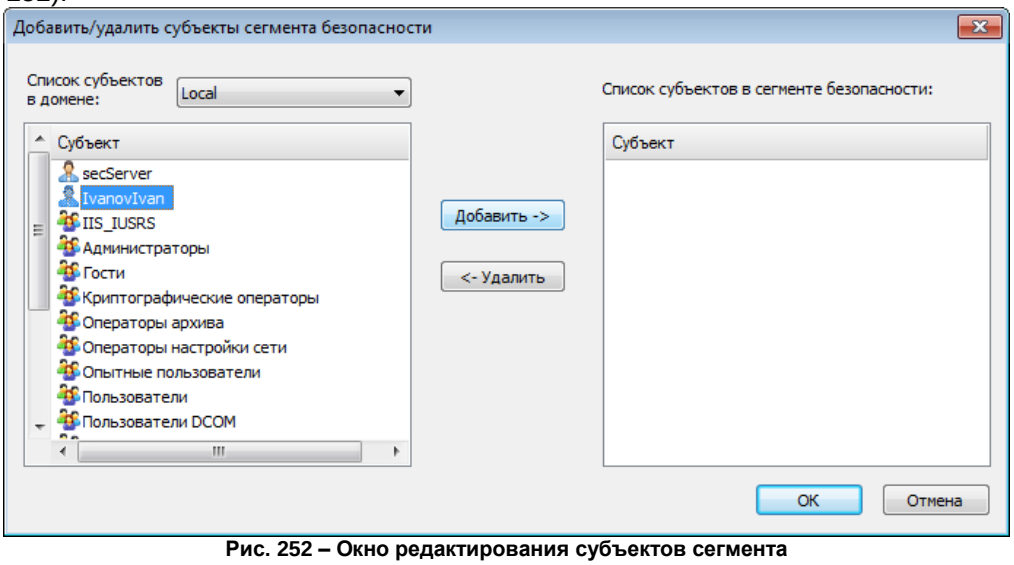


Рис. 252 – Окно редактирования субъектов сегмента

5. Чтобы удалить субъект, необходимо выделить его в «Списке субъектов в группе» и нажать кнопку «Удалить», соответственно (рис. 253).

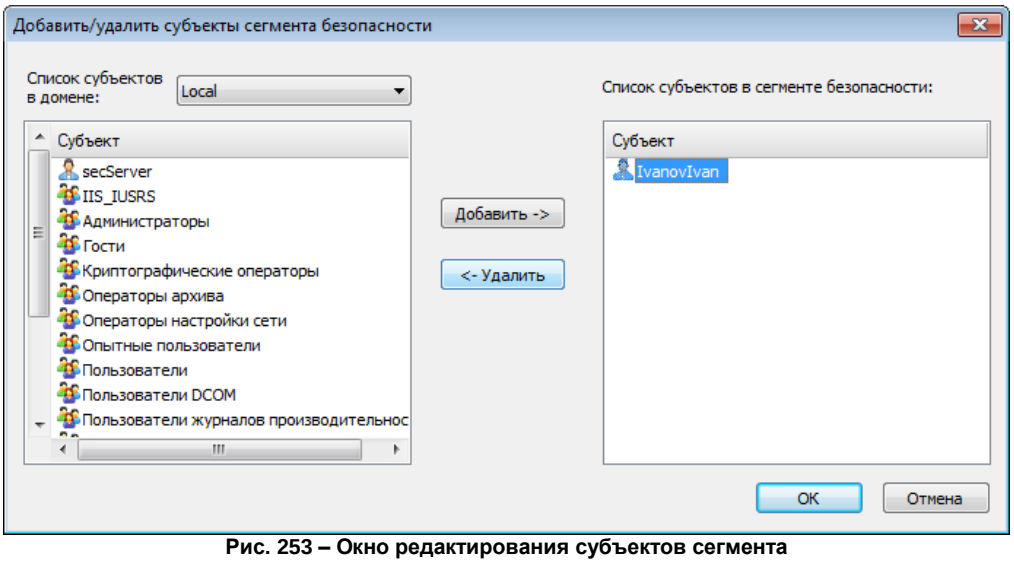


Рис. 253 – Окно редактирования субъектов сегмента

6. После завершения редактирования субъектов группы нажать кнопку «ОК».
7. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

6.6.1.3 Добавление объекта ВИ в сегмент безопасности

Для добавления объекта ВИ в сегмент безопасности необходимо:

1. Перейти на уровень объекта ВИ, например, ВМ.
2. В блоке действия нажать кнопку «Сегмент безопасности» (рис. 254) или выбрать соответствующий пункт в контекстном меню (рис. 255).

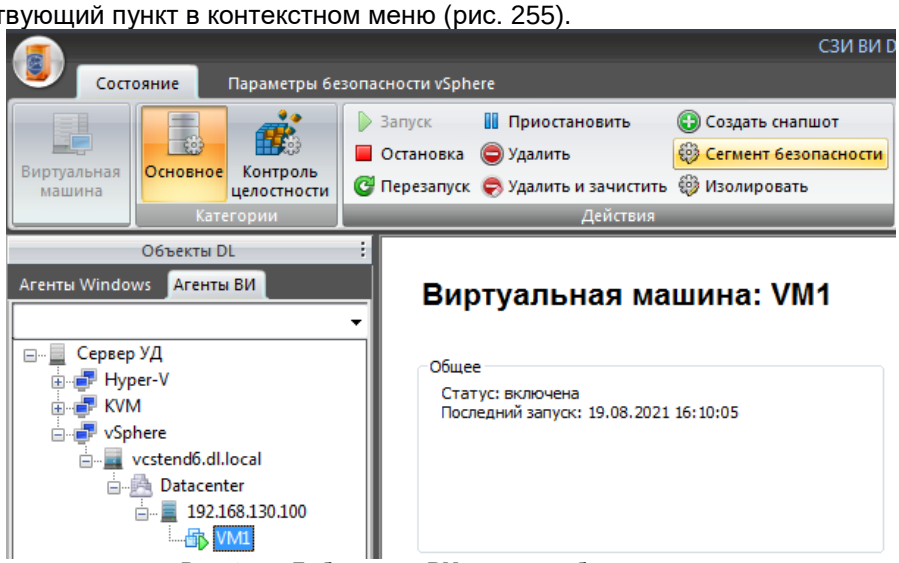


Рис. 254 – Добавление ВМ в сегмент безопасности

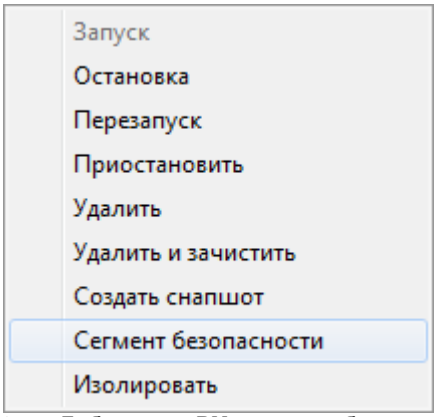


Рис. 255 – Добавление ВМ в сегмент безопасности

3. В появившемся окне выбрать нужный сегмент из выпадающего списка (рис. 256).

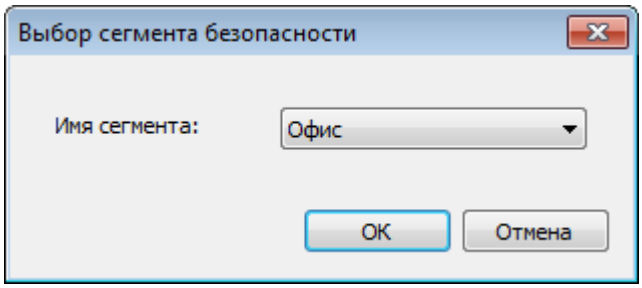


Рис. 256 – Выбор сегмента безопасности

4. Нажать кнопку «ОК».
5. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

6.6.1.4 Удаление объекта ВИ из сегмента безопасности

1. Порядок действий для удаления объекта ВИ из сегмента безопасности аналогичен п. 6.6.1.3, за исключением того, что в окне выбора сегмента безопасности в выпадающем списке необходимо выбрать пункт «Не задан» (рис. 257).

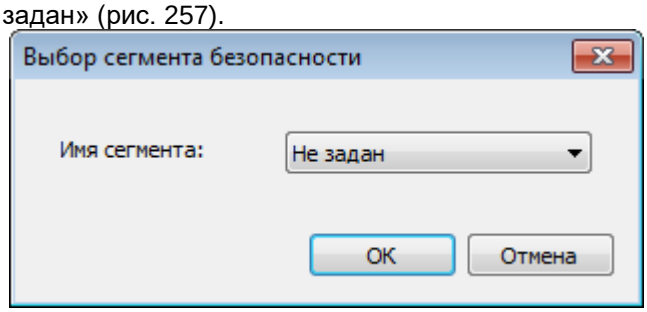


Рис. 257 – Удаление из сегмента безопасности

2. Нажать кнопку «ОК».
3. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

6.6.1.5 Редактирование сегмента безопасности

Для редактирования сегмента безопасности необходимо:

1. Открыть категорию «Состояние» → «Сегменты безопасности».
2. Выбрать в списке необходимый сегмент безопасности.
3. Нажать кнопку «Изменить» в блоке «Действия с сегментами» либо двойным кликом мыши вызвать окно редактирования параметров сегмента безопасности.
4. После внесения изменений нажать кнопку «ОК».
5. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

6.6.1.6 Удаление сегмента безопасности

Для удаления сегмента безопасности необходимо:

1. Открыть категорию «Состояние» → «Сегменты безопасности».
2. Выбрать в списке необходимый сегмент безопасности.
3. Нажать кнопку «Удалить».
4. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

6.6.2 Сегмент безопасности с изолированной ВМ

В отличие от стандартного сегмента безопасности, в сегмент безопасности с изолированной ВМ может входить только одна учетная запись и одна ВМ.

6.6.2.1 Создание сегмента безопасности с изолированной ВМ

При создании сегмента безопасности с изолированной ВМ создание метки безопасности происходит автоматически.

Примечание. Рекомендуется назначать пользователя для работы с изолированной ВМ с правами только на чтение. Для этого можно воспользоваться упрощенным механизмом назначения прав доступа (подробнее см. п.6.4.5.4 «Упрощенное назначение прав доступа пользователям»).

Для создания сегмента безопасности с изолированной ВМ необходимо:

1. Выбрать ВМ.
2. Открыть категорию «Состояние» → «Основное».
3. Нажать кнопку «Изолировать» в блоке «Действия с сегментами» (рис. 258) или воспользоваться контекстным меню (рис. 259).

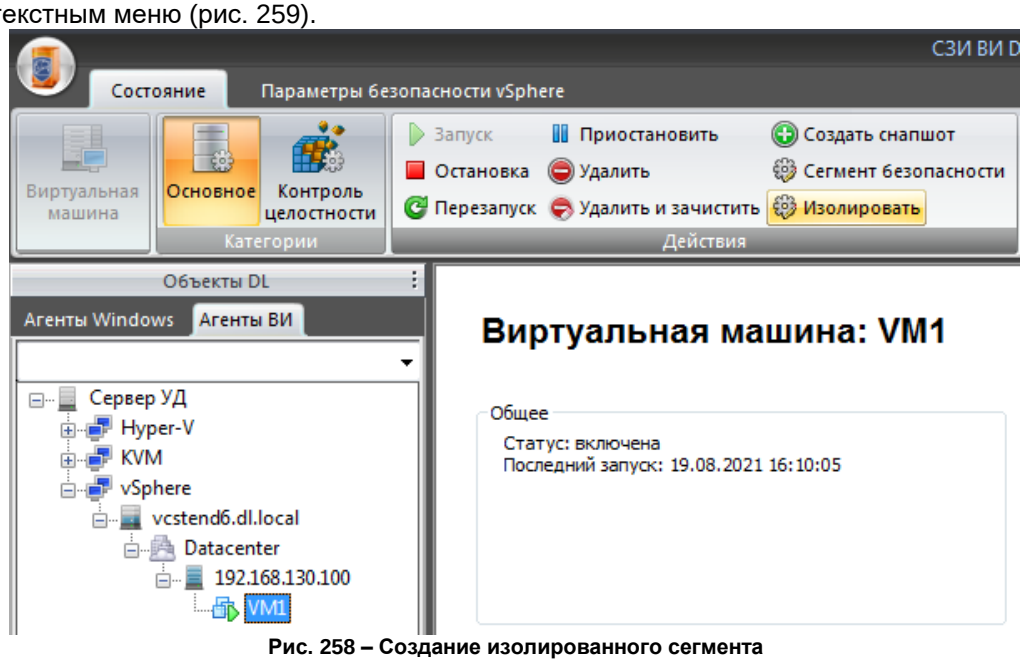


Рис. 258 – Создание изолированного сегмента

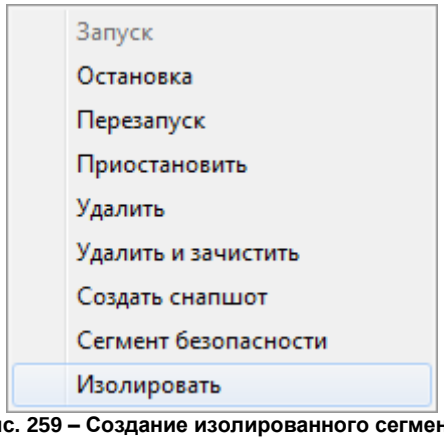


Рис. 259 – Создание изолированного сегмента

4. В появившемся окне выбрать домен и пользователя, которому будет разрешена работа с ВМ, после чего нажать кнопку «ОК». (рис. 260).

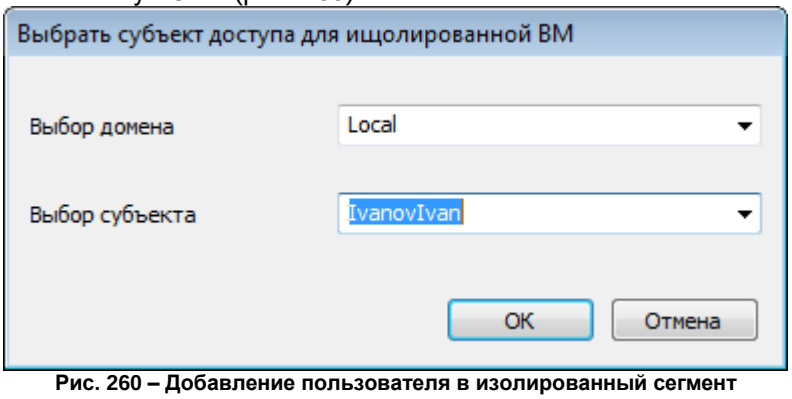


Рис. 260 – Добавление пользователя в изолированный сегмент

5. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

6.6.2.2 Редактирование метки и удаление сегмента безопасности с изолированной ВМ

Редактирование метки безопасности недоступно для сегментов данного типа. При необходимости переназначения учетной записи для доступа к ВМ необходимо заново создать сегмент с изолированной ВМ (см. п. 6.6.2.1).

6.7 Управление сессиями консолей ВМ

СЗИ ВИ позволяет контролировать сессии пользователей при работе с ВМ в средах виртуализации vSphere[24] и Hyper-V[25].

Для того чтобы заблокировать или разблокировать сессию необходимо:

1. Перейти на уровень группы vSphere/Hyper-V и открыть категорию «Состояние» → «Сессии консолей ВМ» (рис. 261).

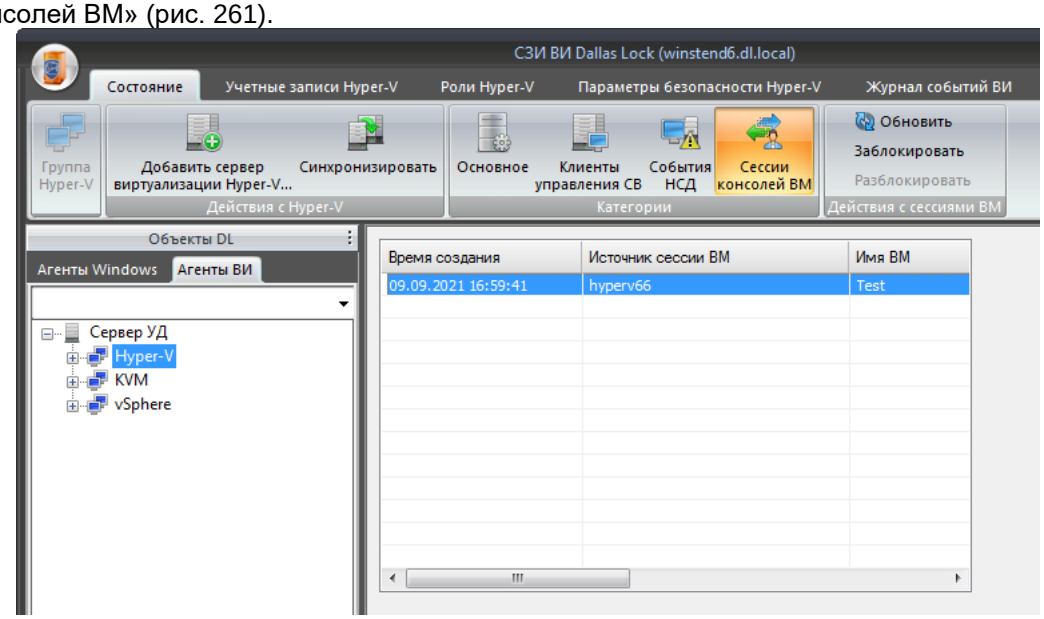


Рис. 261 – Сессии консолей ВМ

2. Выбрать из списка сессию и нажать соответствующую кнопку «Заблокировать» или «Разблокировать».

[24] Данная функция поддерживается для версий ESXi 6.5 и выше.

[25] Для среды виртуализации Hyper-V принудительное прерывание и блокировка сессии пользователя доступно только при работе с ВМ локально и непосредственно с гипервизора Hyper-V с установленными компонентами защиты СЗИ ВИ «Dallas Lock». Прерывание сессий при работе с VMM/Cluster недоступно.

7 ПОДСИСТЕМА КОНТРОЛЯ ЦЕЛОСТНОСТИ

СЗИ ВИ включает в свой состав подсистему обеспечения целостности. Она позволяет контролировать целостность программно-аппаратной среды компьютера, целостность объектов файловой системы и реестра, целостность файлов гипервизора и виртуальных машин, а также восстанавливать файлы и ветки реестры в случае обнаружения нарушенной целостности.

Основу механизмов контроля целостности представляет проверка соответствия контролируемого объекта эталонному образцу. Для этого используются контрольные суммы.

Процедура контроля целостности осуществляется следующим образом: после назначения дескриптора целостности при следующей проверке проверяется, было ли уже вычислено эталонное значение контрольной суммы параметра. Если оно еще не было вычислено, оно вычисляется и сохраняется. Если же оно уже было вычислено, то оно сравнивается с вычисляемым текущим значением контрольной суммы контролируемого параметра. Если хотя бы для одного из проверяемых параметров текущее значение параметра не совпало с эталонным значением, результат проверки считается отрицательным, а целостность контролируемых объектов – нарушенной.

Для программного-аппаратного контроля целостности клиентов Windows СЗИ ВИ использует подсистему WMI. Если стороннее ПО блокирует или встраивается в работу этой подсистемы, могут наблюдаться проблемы выполнения расчета программно-аппаратной целостности и, соответственно, проблемы авторизации пользователей.

Внимание! Следует избегать установки Microsoft SQL сервера в конфигурации, при которой он будет запускаться от имени пользователя. Данный вариант приводит к взаимоблокировке подсистемы WMI и SQL-сервера. Это, в свою очередь, может сопутствовать проблемам авторизации пользователей в ОС.

В ряде случаев для разрешения сценариев блокировки сессий на этапе авторизации может помочь использование сессий-исключений (подробнее см. п. 5.1.2.4 «Сессии-исключения»). Для сессий-исключений обращение к подсистеме WMI в рамках встроенных механизмов СЗИ не производится.

У каждой учетной записи пользователя Windows есть свойство, отвечающее за то, что делать при выявлении нарушения целостности – либо блокировать загрузку (при условии, что в свойствах учетной записи включен параметр «Запретить работу при нарушении целостности»), либо выдавать предупреждение и продолжать загрузку.

Проверка целостности по умолчанию осуществляется при загрузке компьютера, при доступе к объекту и при проверке по команде администратора. Дополнительно можно задать проверку целостности по расписанию и по времени.

Примечание. Для расчета контрольных сумм по содержимому объектов используются алгоритмы: CRC32, MD5. Алгоритм выбирается администратором при назначении контроля целостности.

Для изменения значений параметров контроля целостности и для изменения списка контролируемых объектов: файловой системы, программно-аппаратной среды и веток реестра (добавление, удаление, редактирование), пользователь должен обладать правом «Параметры безопасности: управление». В то же время для просмотра только значений установленных параметров и дескрипторов целостности пользователь должен обладать правом «Параметры безопасности: просмотр».

Примечание. СЗИ ВИ для возможности восстановления веток реестра при нарушении контроля целостности требуется доступ к соответствующим веткам от имени системного пользователя. Если доступ системному пользователю будет ограничен, функциональная возможность восстановления веток не будет работать корректно.

7.1 Контроль целостности файлов

События нарушения целостности сопровождаются записью в журнале ЦУ СЗИ ВИ, при этом в графах «Событие» и «Результат» отображается значение параметра контроля целостности.

Внимание! Перед запуском ВМ необходимо проверить КЦ файлов данной ВМ.

Примечание. В случае обнаружения события нарушения целостности, на ПК с запущенной Консолью будет отправляться соответствующее событие сигнализации (см. п. 3.6 «Сигнализация об НСД»).

7.1.1 Настройка контроля целостности СВ vSphere

Настройка политик и параметров КЦ в части ОС Windows описана в п. 7.3 «Настройка параметров контроля целостности для клиентов Windows».

Настройка параметров КЦ в части ВМ описана в п. 7.2 «Настройка контроля целостности ВМ».

7.1.2 Настройка контроля целостности СВ vCSA

Для системных файлов и аппаратного обеспечения СВ vCSA КЦ включен по умолчанию и отключить его невозможно, возможно только изменить алгоритм расчета КС.

Просмотр списка системных файлов взятых под КЦ для СВ vCSA происходит на уровне СВ в категории «Состояние» → «Контроль целостности» в подкатегории «Все» или «vCSA» (рис. 262).

Настройка параметров КЦ в части ВМ описана в п. 7.2 «Настройка контроля целостности ВМ».

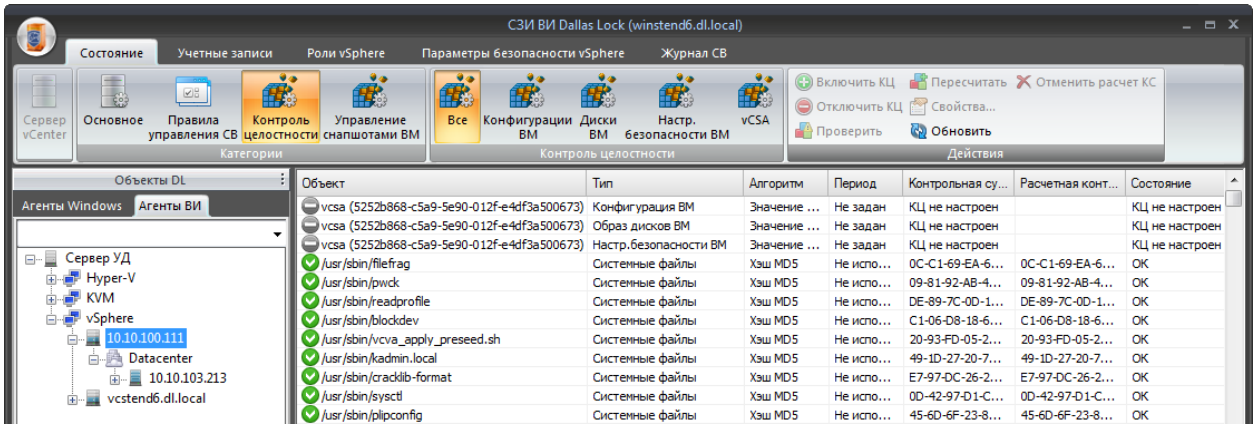


Рис. 262 – КЦ системных файлов и аппаратного обеспечения vCSA

Частота периодической проверки КЦ системных файлов гипервизора ESXi редактируется только для всех гипервизоров (см. п. 3.3.3 «Основные параметры группы СВ vSphere»).

7.1.3 Настройка контроля целостности гипервизора ESXi

Для системных файлов и аппаратного обеспечения гипервизора ESXi КЦ включен по умолчанию и отключить его невозможно, возможно только изменить алгоритм расчета КС.

Просмотр списка системных файлов взятых под КЦ для гипервизора ESXi происходит на уровне гипервизора в категории «Состояние» → «Контроль целостности» в подкатегории «Все» или «ESXi» (рис. 263).

Настройка параметров КЦ в части ВМ описана в п. 7.2 «Настройка контроля целостности ВМ».

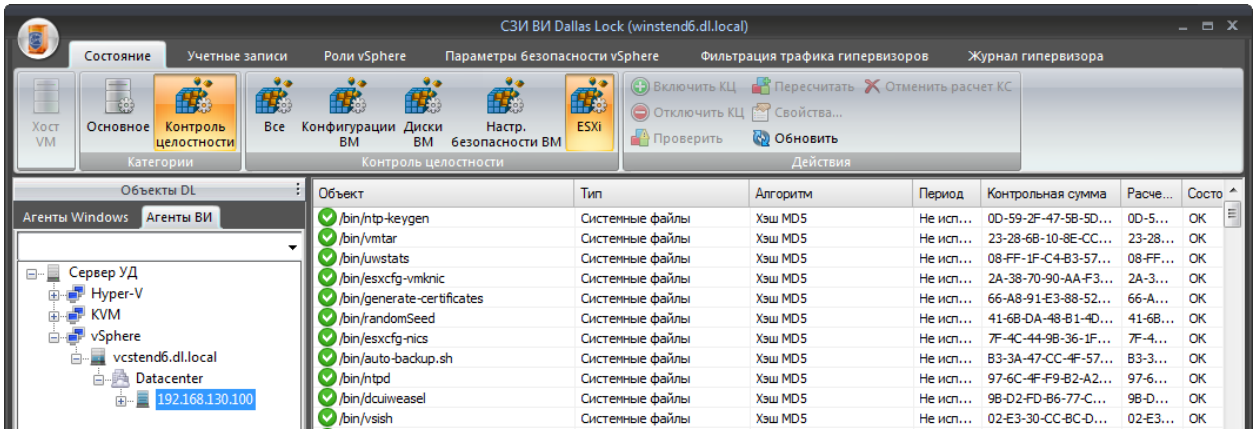


Рис. 263 – КЦ системных файлов ESXi

Просмотр списка КЦ аппаратного обеспечения гипервизоров ESXi происходит на уровне СВ или гипервизора в категории «Состояние» → «Контроль целостности» → «Все» или «ESXi» (рис. 264).

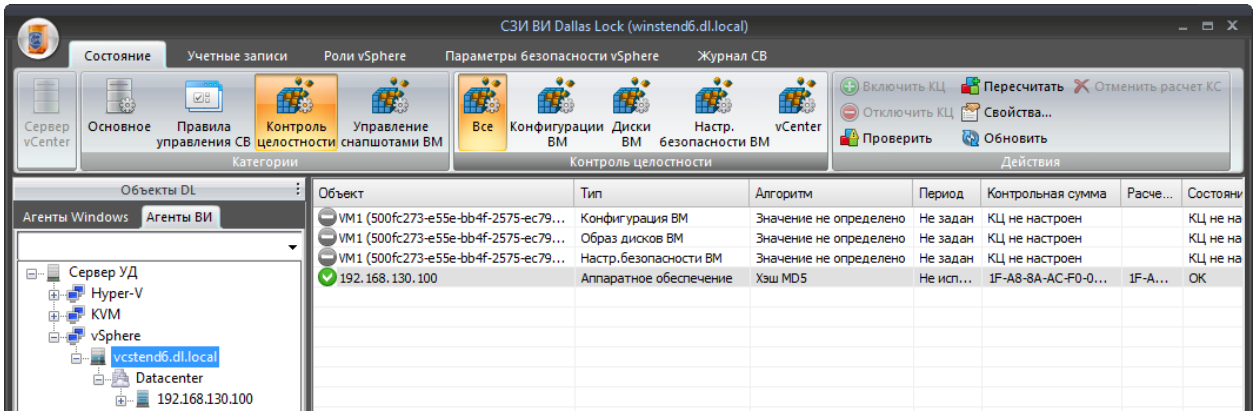


Рис. 264 – КЦ аппаратного обеспечения ESXi

Примечание. При проведении КЦ аппаратной среды СЗИ ВИ получает от гипервизора ESXi набор данных об аппаратном окружении гипервизора. Однако, гипервизор ESXi не передает данные о подключении/отключении некоторых USB-устройств (например, таких устройств ввода-вывода, как клавиатура или мышь). В связи с этим предупреждение о нарушении КЦ аппаратной среды при подключении/отключении таких устройств не выводится.

Примечание. При подключении/отключении flash-накопителей предупреждение о нарушении КЦ на гипервизоре ESXi выводится при первой проверке КЦ и при последующих перезагрузках платформы.

Частота периодической проверки КЦ системных файлов гипервизора ESXi редактируется только для всех гипервизоров (см. п. 3.3.3 «Основные параметры группы СВ vSphere»).

7.1.4 Настройка контроля целостности СВ Hyper-V

Настройка политик и параметров КЦ описана в п. 7.3 «Настройка параметров контроля целостности для клиентов Windows».

Настройка параметров КЦ в части ВМ описана в п. 7.2 «Настройка контроля целостности ВМ».

7.1.5 Настройка контроля целостности гипервизора KVM

Для системных файлов и аппаратного обеспечения гипервизора KVM КЦ включен по умолчанию и отключить его невозможно, возможно только изменить алгоритм расчета КС.

Просмотр списка системных файлов взятых под КЦ для гипервизора KVM происходит на уровне гипервизора в категории «Состояние» → «Контроль целостности» в подкатегории «Все» или «Система» (рис. 265).

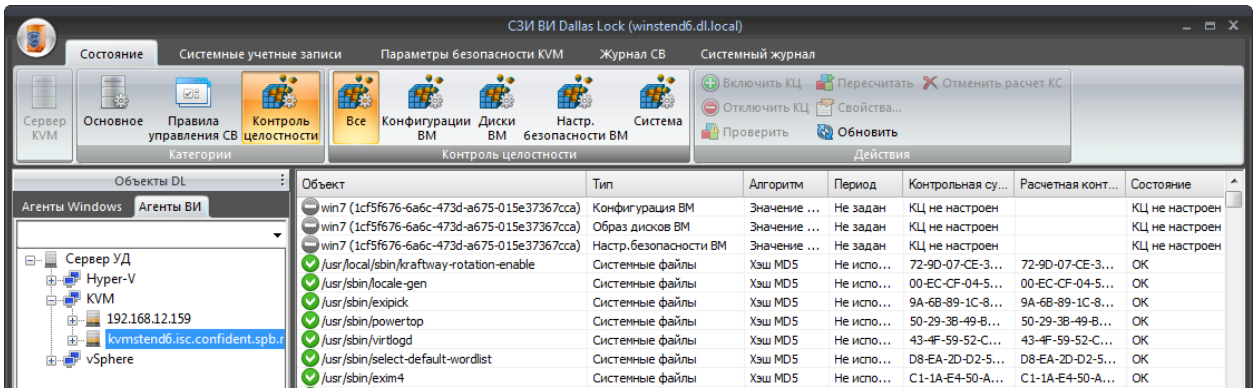


Рис. 265 – КЦ системных файлов гипервизора KVM

Частота периодической проверки КЦ системных файлов гипервизора KVM редактируется только для всех объектов группы KVM (см. п. 3.3.5 «Основные параметры группы KVM»).

Настройка параметров КЦ в части ВМ описана в п. 7.2 «Настройка контроля целостности ВМ».

7.1.6 Настройка контроля целостности СВ oVirt/zVirt/HOSTVM/РЕД Вирт

Для системных файлов и аппаратного обеспечения СВ oVirt/zVirt/HOSTVM/РЕД Вирт КЦ включен по умолчанию и отключить его невозможно, возможно только изменить алгоритм расчета КС.

Просмотр списка системных файлов взятых под КЦ для СВ oVirt/zVirt/HOSTVM/РЕД Вирт происходит на уровне СВ в категории «Состояние» → «Контроль целостности» в подкатегории «Все» или «Система» (рис. 266).

Настройка параметров КЦ в части ВМ описана в п. 7.2 «Настройка контроля целостности ВМ».

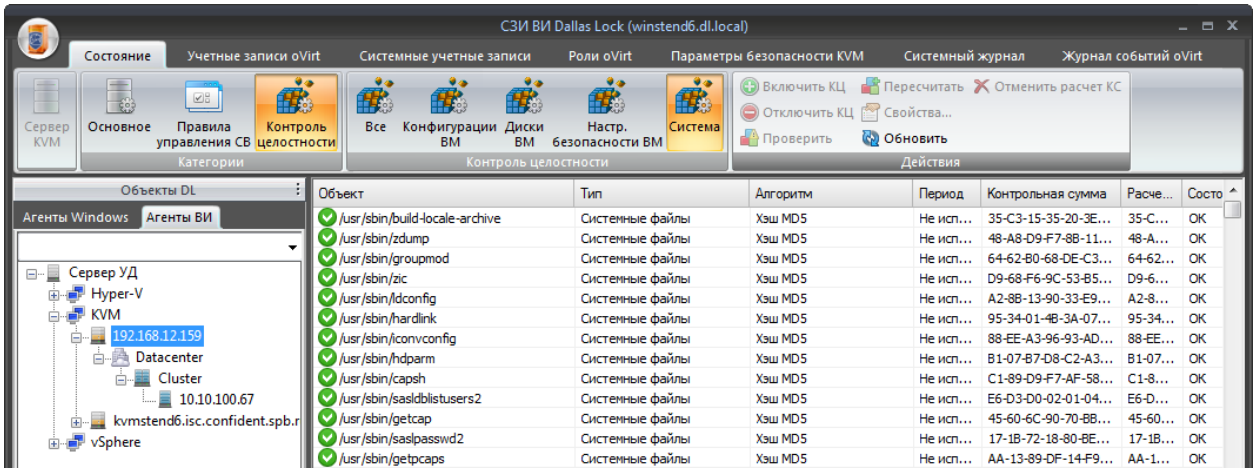


Рис. 266 – КЦ системных файлов СВ oVirt/zVirt/HOSTVM/РЕД Вирт

Частота периодической проверки КЦ системных файлов и аппаратного обеспечения СВ oVirt/zVirt/HOSTVM/РЕД Вирт редактируется только для всех объектов группы KVM (см. п. 3.3.5 «Основные параметры группы KVM»).

7.1.7 Настройка контроля целостности гипервизора oVirt/zVirt/HOSTVM/РЕД Вирт

Для системных файлов и аппаратного обеспечения гипервизора oVirt/zVirt/HOSTVM/РЕД Вирт КЦ включен по умолчанию и отключить его невозможно, возможно только изменить алгоритм расчета КС.

Просмотр списка системных файлов взятых под КЦ для гипервизора oVirt/zVirt/HOSTVM/РЕД Вирт происходит на уровне гипервизора в категории «Состояние» → «Контроль целостности» (рис. 267).

Настройка параметров КЦ в части ВМ описана в п. 7.2 «Настройка контроля целостности ВМ».

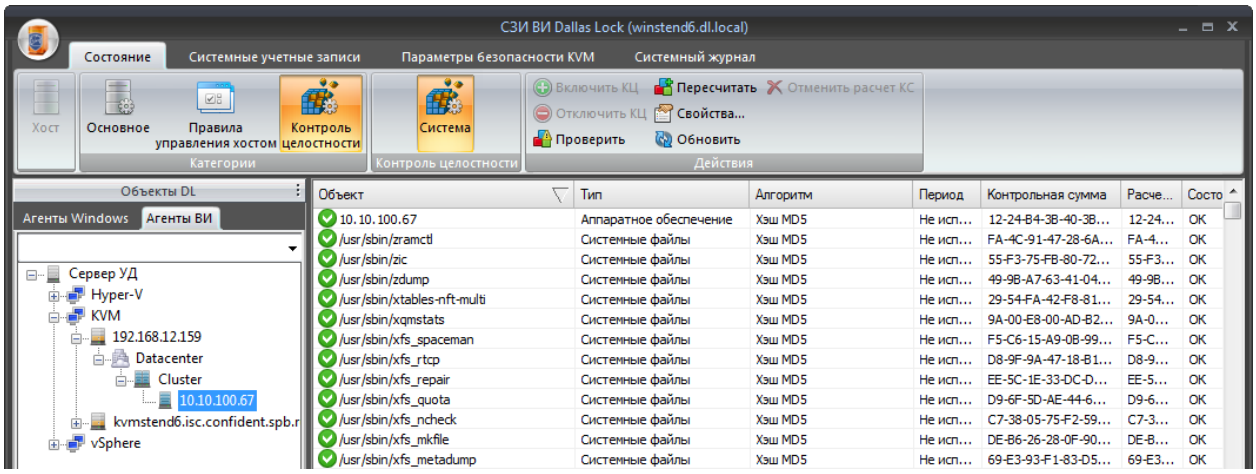


Рис. 267 – КЦ системных файлов гипервизора oVirt/zVirt/HOSTVM/РЕД Вирт

Частота периодической проверки КЦ системных файлов и аппаратного обеспечения гипервизора oVirt/zVirt/HOSTVM/РЕД Вирт редактируется только для всех объектов группы KVM (см. п. 3.3.5 «Основные параметры группы KVM»).

7.2 Настройка контроля целостности ВМ

Внимание! При выполнении миграции ВМ между хостами КЦ автоматически не пересчитывается и регистрируется событие НСД. Для исключения подобных ситуаций необходимо перед миграцией ВМ снять КЦ с данной ВМ, после завершения миграции поставить необходимые компоненты ВМ под КЦ.

7.2.1 Настройка контроля целостности конфигурации ВМ

Проверка КЦ конфигурации ВМ осуществляется периодически и при включении ВМ. Частота периодической проверки КЦ для конфигурации ВМ редактируется при настройке КЦ для конфигурации ВМ.

Для включения контроля целостности конфигурации ВМ необходимо:

1. Выбрать уровень Сервера виртуализации Hyper-V, vSphere, KVM или oVirt/zVirt/HOSTVM/РЕД Вирт, либо выбрать уровень гипервизора или ВМ и открыть вкладку «Состояние» → «Контроль целостности» → «Конфигурации ВМ».
2. Выбрать из списка виртуальную машину.
3. Выбрать действие «Включить КЦ» (рис. 268).

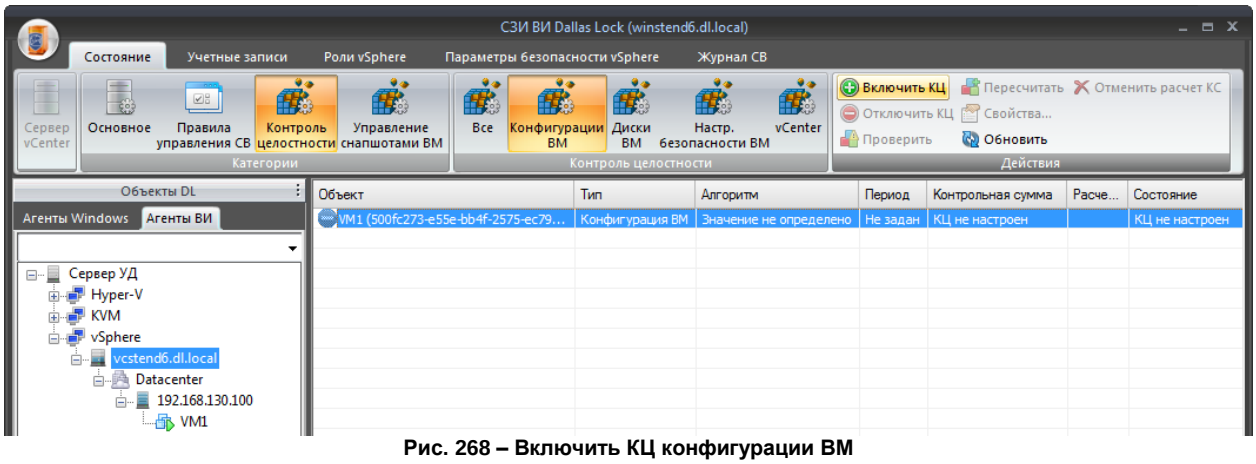


Рис. 268 – Включить КЦ конфигурации ВМ

4. Выбрать алгоритм расчета контрольной суммы (CRC32, Хэш MD5) (рис. 269).

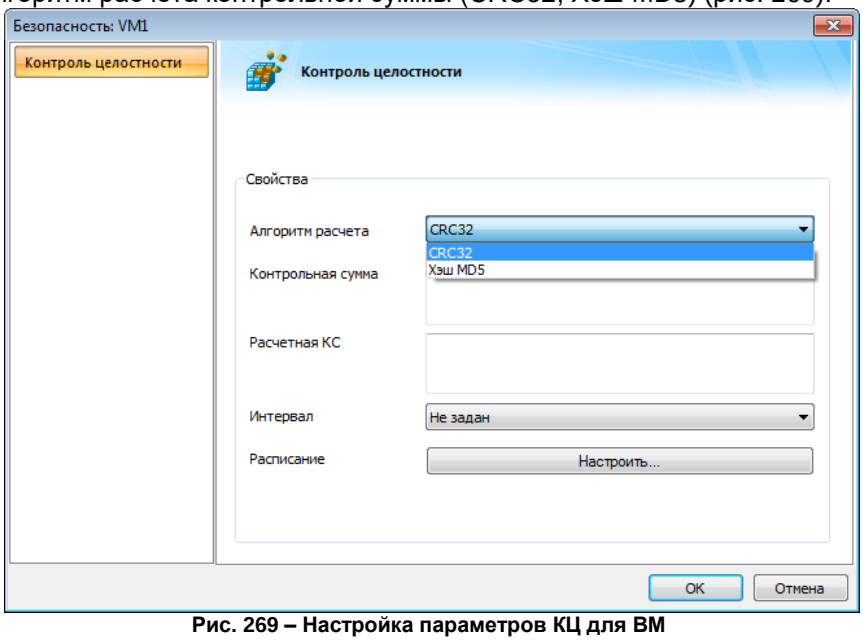


Рис. 269 – Настройка параметров КЦ для ВМ

5. Выбрать интервал расчета (периодичность проверки).
6. Настроить расписание.
7. Нажать кнопку «ОК».
8. После завершения расчета КС, появится соответствующее информационное окно.

Для снятия КЦ необходимо выбрать объект с включенным КЦ и на панели действий нажать кнопку «Отключить КЦ».

7.2.2 Настройка контроля целостности для образов дисков ВМ

Проверка КЦ образов дисков ВМ осуществляется периодически и при включении ВМ. Частота периодической проверки КЦ для образов дисков ВМ редактируется при настройке КЦ для образов дисков ВМ.

Примечание. Расчет контрольных сумм образов дисков ВМ происходит только при выключенной ВМ.

Для включения контроля целостности для образов дисков ВМ необходимо:

1. Выбрать уровень Сервера виртуализации, либо выбрать уровень гипервизора или ВМ и открыть КЦ «Состояние» → «Контроль целостности» → «Диски ВМ».
2. Выбрать из списка образ диска ВМ.
3. Выбрать действие «Включить КЦ».
4. Выбрать алгоритм расчета контрольной суммы (CRC32, Хэш MD5).
5. Выбрать интервал расчета (периодичность проверки).
6. Настроить расписание.
7. Нажать кнопку «ОК».
8. Появится предупреждающее окно, что выполняется расчет КС (рис. 270). Данное операция может занимать некоторое время в зависимости от объемов дисков ВМ.

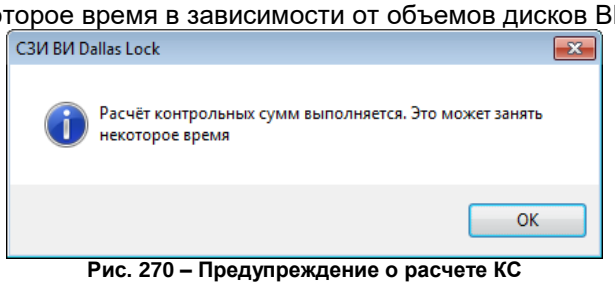


Рис. 270 – Предупреждение о расчете КС

9. Нажать кнопку «ОК».
10. После завершения расчета КС, появится соответствующее информационное окно, а также всплывающее сообщение на панели уведомлений Windows.

Для снятия КЦ необходимо выбрать объект с включенным КЦ и на панели действий нажать кнопку «Отключить КЦ».

Примечание. КЦ BIOS ВМ производится за счет обнаружения изменений файла *.nvram данной ВМ. Проверка целостности файла *.nvram осуществляется во время КЦ образов дисков ВМ данной ВМ, когда она выключена. В случае, если изменение такого файла производится авторизовавшимся при доступе к ВМ пользователем, изменения в файле *.nvram считаются легитимными и предупреждение о нарушении КЦ данного файла не выводится.

Примечание. В случае возникновении ошибки постановки ВМ под КЦ, находящейся в кластере Hyper-V, необходимо убедиться в корректности установленных атрибутов владельца в настройках ВМ в кластере.

7.2.3 Настройка контроля целостности настроек безопасности ВМ

Проверка КЦ настроек безопасности ВМ[26] осуществляется периодически и при включении ВМ. Частота периодической проверки КЦ для настроек безопасности ВМ редактируется при настройке КЦ для настроек безопасности ВМ.

Для включения контроля целостности для образов дисков ВМ необходимо:

1. Выбрать уровень Сервера виртуализации, либо выбрать уровень гипервизора или ВМ и открыть КЦ «Состояние» → «Контроль целостности» → «Настройки безопасности ВМ».

[26] Данный параметр не доступен для платформ виртуализации на базе KVM (KVM/oVirt/zVirt/HOSTVM).

2. Выбрать из списка настройки безопасности ВМ.
3. Выбрать действие «Включить КЦ».
4. Выбрать алгоритм расчета контрольной суммы (CRC32, Хэш MD5).
5. Выбрать интервал расчета (периодичность проверки).
6. Настроить расписание.
7. Нажать кнопку «ОК».
8. После завершения расчета КС, появится соответствующее информационное окно, а также всплывающее сообщение на панели уведомлений Windows.

Для снятия КЦ необходимо выбрать объект с включенным КЦ и на панели действий нажать кнопку «Отключить КЦ».

7.2.4 Проверка целостности конфигураций, дисков ВМ и настроек безопасности ВМ

Если некоторый объект, на который назначена целостность, будет изменен или поврежден, то при нажатии на кнопку «Проверить» (рис. 271), в списке объектов контроля целостности, значок выбранного объекта у которого нарушена целостность изменится на красный .

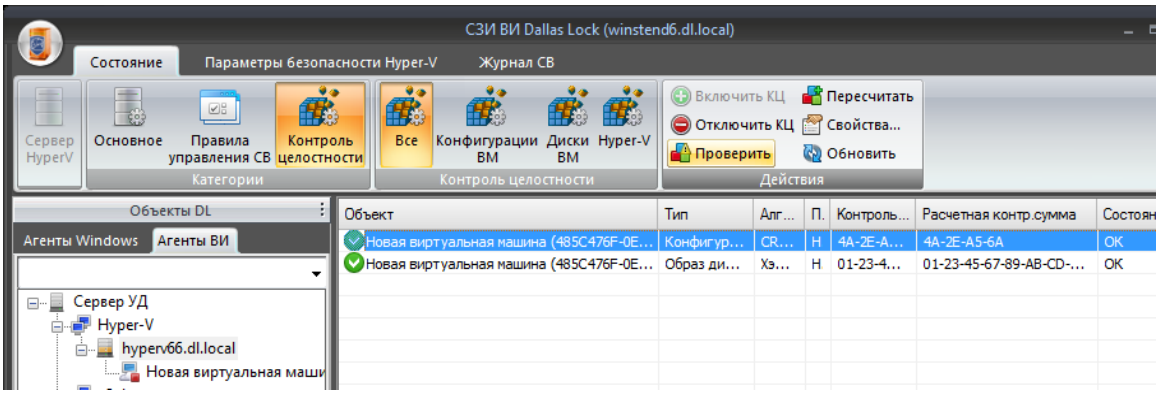


Рис. 271 – Контроль целостности конфигураций и дисков ВМ

При нажатии кнопки «Пересчитать» происходит пересчет контрольной суммы. Пересчет контрольной суммы позволяет принять текущее состояние файла за эталонное и соответственно снять нарушение КЦ.

Значения контрольных сумм для контролируемых объектов в Консоли появляются после команд проверки и пересчета контрольных сумм.

Примечание. Подсчет контрольной суммы образа дисков ВМ производится с учетом всех используемых в работе ВМ жестких дисков. Вне зависимости от их количества, результатом будет одна контрольная сумма. Нарушение целостности одного из дисков повлечет за собой событие нарушения целостности образа дисков ВМ.

Внимание! При совпадении факта изменения конфигурации ВМ с периодическим контролем целостности конфигурации ВМ, изменение конфигурации может быть заблокировано, о чем будет сообщено в журнале VMware. Повторное изменение конфигурации должно быть успешным.

7.3 Настройка параметров контроля целостности для клиентов Windows

Глобальная настройка параметров КЦ клиентов Windows производится в дереве «Агенты Windows» на уровне Сервера УД. Данные настройки наследуются всеми клиентами по умолчанию.

7.3.1 Настройка политик контроля целостности

Для настройки политик КЦ необходимо:

1. Перейти в «Параметры безопасности домена» → «Политики» (рис. 272).

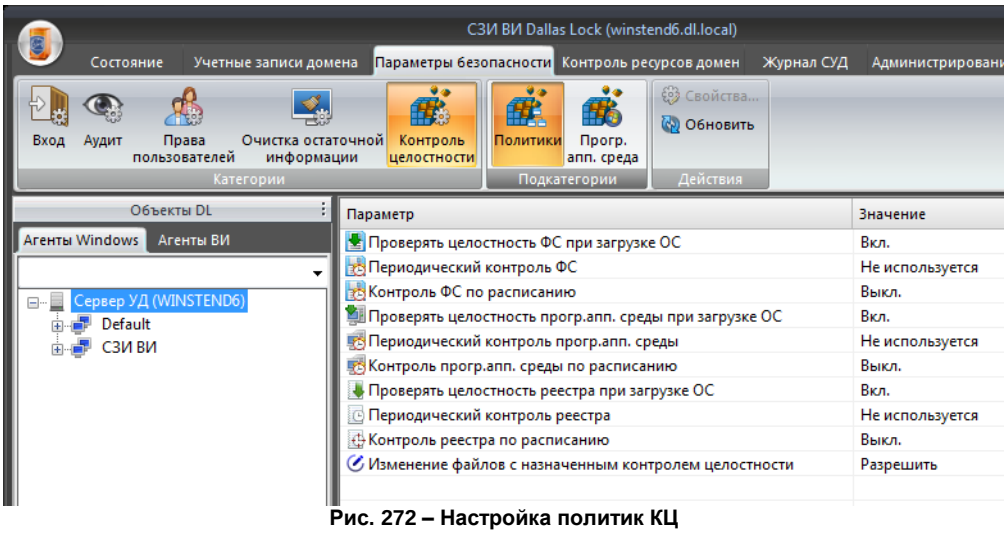


Рис. 272 – Настройка политик КЦ

2. Выбрать параметр, на панели «Действия» нажать кнопку «Свойства», либо двойным кликом мыши вызвать окно редактирования параметров безопасности.
3. Установить необходимое значение и нажать кнопку «ОК» (рис. 273), либо «Применить» (рис. 274) в зависимости от настраиваемого параметра.

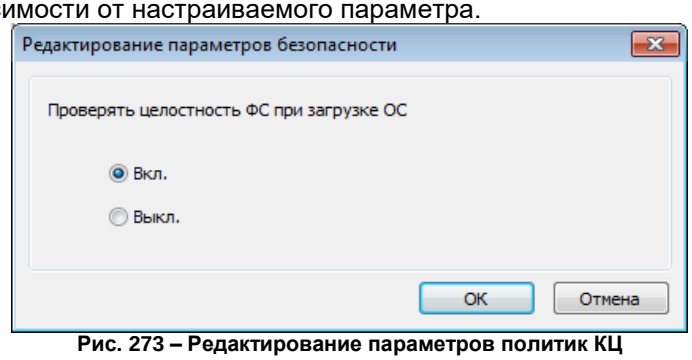


Рис. 273 – Редактирование параметров политик КЦ

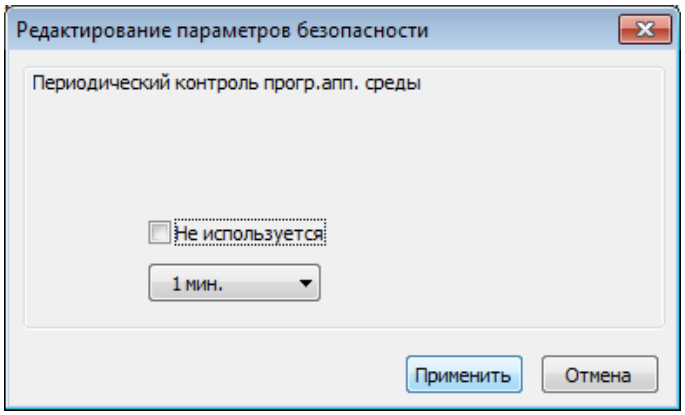


Рис. 274 – Редактирование параметров политик КЦ

4. Перейти на вкладку «Состояние» и нажать кнопку «Синхронизировать».

7.3.2 Настройка контроля целостности программно-аппаратной среды

Для настройки параметров КЦ программно-аппаратной среды необходимо:

1. Перейти в «Параметры безопасности домена» → «Прогр. апп. среда».
2. Выбрать параметр, на панели «Действия» нажать кнопку «Свойства», либо двойным кликом мыши вызвать окно редактирования параметров безопасности.
3. Снять флаг с поля «Не используется», указать необходимый алгоритм подсчета контрольных сумм и нажать кнопку «Применить».
4. Перейти на вкладку «Состояние» и нажать кнопку «Синхронизировать».

7.3.3 Настройка политик контроля целостности для группы

Параметры политики контроля целостности настраиваются в дереве «Агенты Windows» на уровне Сервера УД и наследуются на нижестоящих уровнях. Если необходимо настроить параметры контроля целостности индивидуально для клиента, то необходимо:

1. Перейти в дерево «Агенты Windows».
2. На уровне группы перейти в «Параметры безопасности группы» → «Контроль целостности».
3. Выбрать подкатегорию «Политики» (рис. 275).

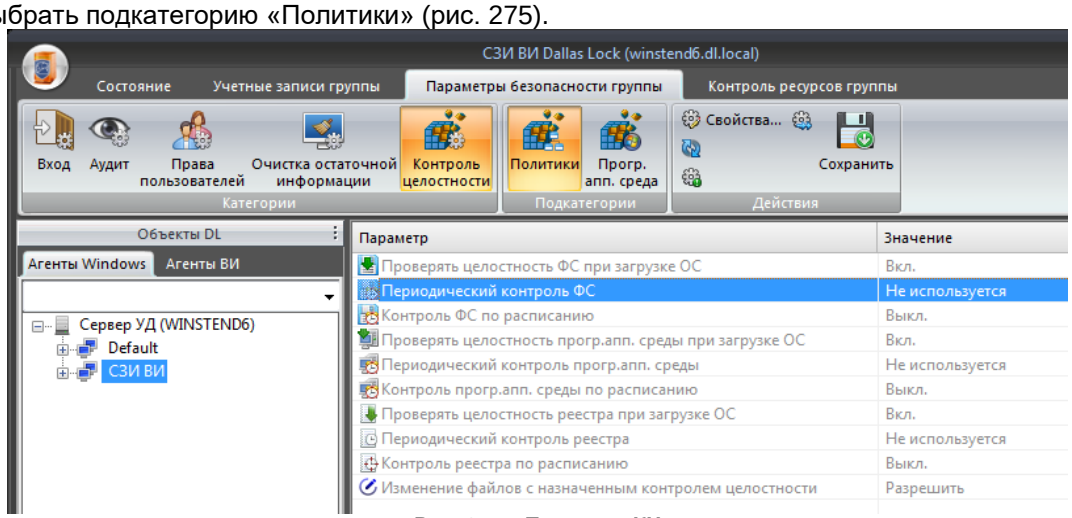


Рис. 275 – Политики КЦ

4. Выбрать настраиваемый параметр, на панели «Действия» нажать кнопку «Свойства». В случае если необходимо установить отличное от наследуемого значение, следует убрать флажки из полей «Наследуется» и «Не используется» и индивидуально установить алгоритм расчета контрольной суммы для данного параметра (рис. 276).

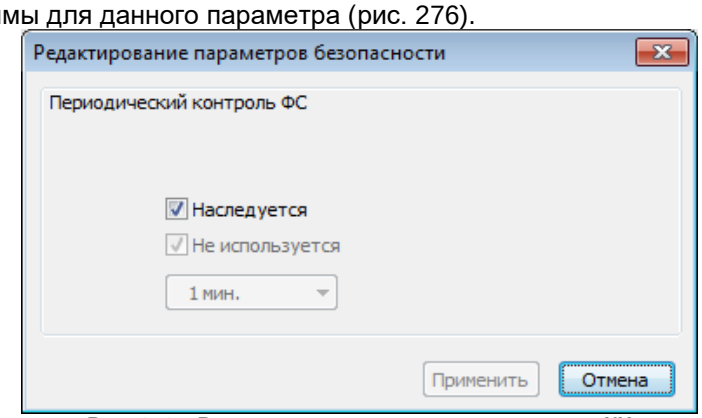


Рис. 276 – Редактирование параметров политик КЦ

После изменения параметра нажать кнопку «Применить».

5. В категории «Действия» нажать кнопку «Сохранить».
6. Перейти на вкладку «Состояние» и нажать кнопку «Синхронизировать».

7.3.4 Настройка параметров контроля целостности программно-аппаратной среды для группы

С помощью политик контроля целостности на вкладке «Параметры безопасности группы» устанавливается периодичность и расписание контроля целостности для объектов программно-аппаратной среды.

Чтобы выбрать категории объектов программно-аппаратной среды, для которых требуется установить контроль целостности, необходимо открыть соответствующую категорию на вкладке «Параметры безопасности группы» → «Контроль целостности»

1. Выбрать подкатегорию «Прогр. апп. среда» (рис. 277).

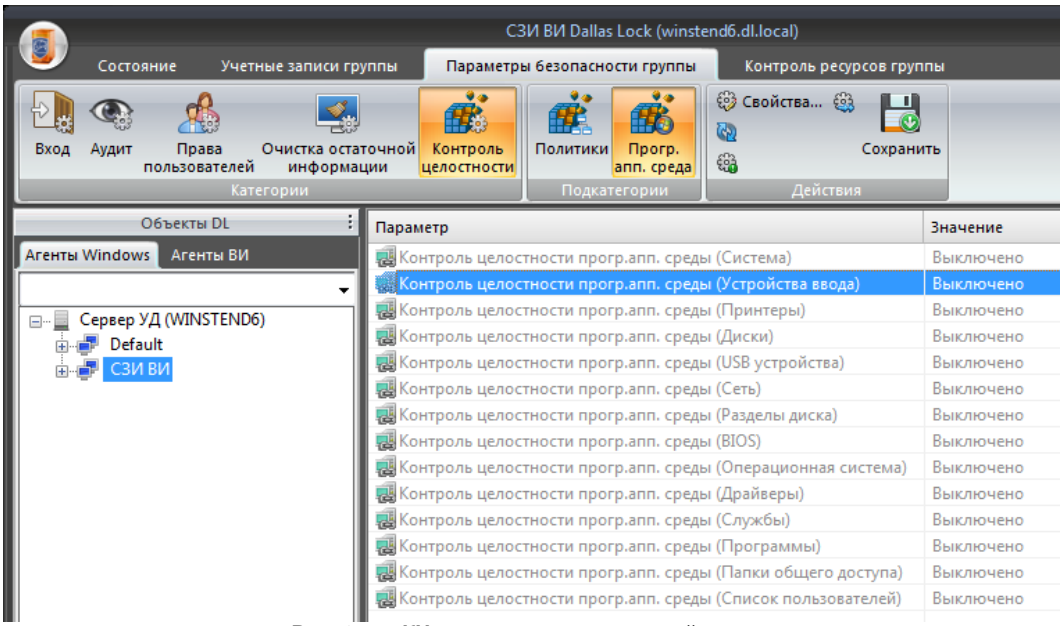


Рис. 277 – КЦ программно-аппаратной среды

2. Выбрать настраиваемый параметр, на панели «Действия» выбрать пункт «Свойства». В случае если необходимо установить отличное от наследуемого значение, следует убрать флажки из полей «Наследуется» и «Не используется» и индивидуально установить алгоритм расчета контрольной суммы для данного параметра.
3. После изменения параметра нажать кнопку «Применить». Затем в категории «Действия» нажать кнопку «Сохранить».
4. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

8 ПОДСИСТЕМА ГАРАНТИРОВАННОЙ ОЧИСТКИ ПАМЯТИ

8.1 Очистка остаточной информации из консоли на клиентах Windows

Очистка остаточной информации производится средствами СЗИ ВИ.

Настройка политик очистки остаточной информации для ВМ клиентов Windows выполняется в дереве «Агенты Windows» на уровне Сервера УД в категории «Параметры безопасности домена» → «Очистка остаточной информации». Для настройки доступны следующие параметры:

- Очищать освобождаемое дисковое пространство;
- Очищать файл подкачки виртуальной памяти;
- Проверять очистку информации;
- Количество циклов затирания;
- Затирающая последовательность.

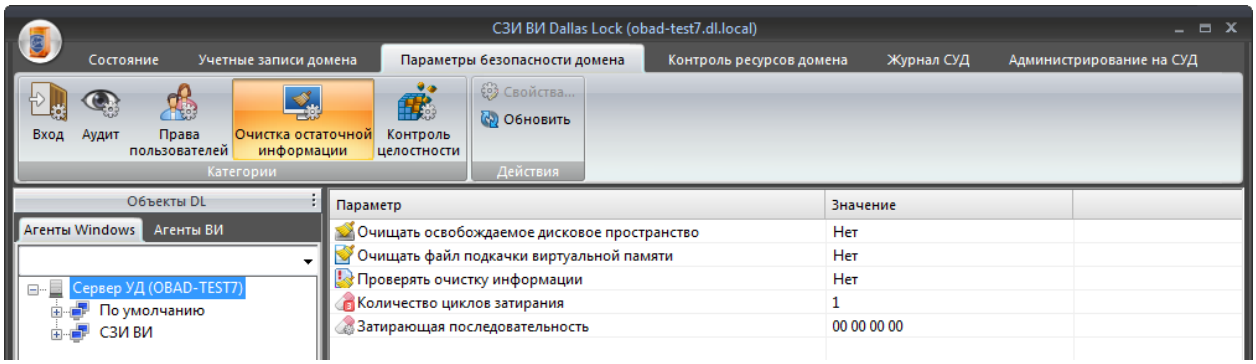


Рис. 278 – Параметры очистки остаточной информации

Редактирование значений данных параметров происходит через окно редактирования параметров безопасности, которое вызывается отдельно для каждого параметра двойным кликом мыши на нем.

Затирание производится записью маскирующей последовательности поверх освобождаемого пространства. Параметру «Количество циклов затирания» можно задать значение от одного до четырех циклов затирания. Чем большее число циклов затирания выбрано, тем надежнее происходит удаление информации. При этом следует учесть, что чем больше циклов затирания будет выбрано, тем больше времени эта процедура будет занимать.

Другим параметром «Затирающая последовательность» определяется метод затирания остаточной информации, путем установки числовых байтовых значений (от 0 до F) для каждого из четырех цикла затирания. Если эти значения не установлены, или установлены не для каждого цикла, то по умолчанию для затирающей последовательности циклов используется последовательность, установленная в СЗИ ВИ.

Установленное количество циклов затирания и методы затирания используются при всех установленных видах очистки остаточной информации: по команде администратора, в автоматическом режиме.

8.1.1 Удаление файлов и зачистка остаточной информации по команде

СЗИ ВИ предоставляет возможность удаления данных без возможности их восстановления на компьютерах с установленным Центром управления СЗИ ВИ Dallas Lock или агентом управления Windows. После установки СЗИ ВИ у каждого объекта файловой системы в контекстном меню появляется дополнительный пункт «СЗИ ВИ: Удалить и зачистить» (рис. 279).

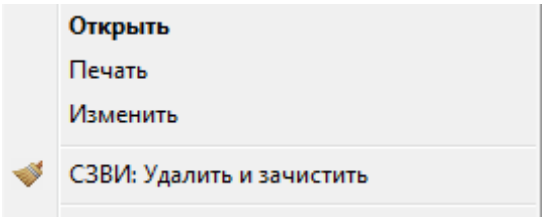


Рис. 279 – Контекстное меню объекта файловой системы

После выбора данного пункта появится окно с требованием подтвердить операцию удаления и зачистки (рис. 280).

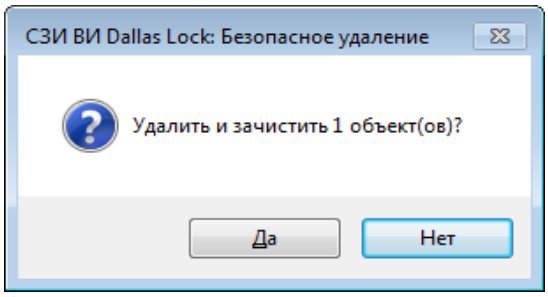


Рис. 280 – Подтверждение удаления файлов

Внимание! Для того чтобы выполнить зачистку логического диска, пользователь от которого выполняется операция должен иметь следующие права:

1. низкоуровневая запись и чтения для данного диска;
2. редактирование политик.

При активации удаления происходит зачистка данного объекта путем перезаписи файла. Количество циклов затирания определяется соответствующей политикой. После перезаписи восстановить значимый фрагмент файла становится практически неосуществимо. После успешного удаления объектов система выведет соответствующее подтверждение (рис. 281).

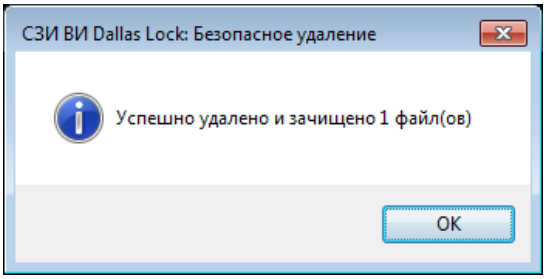


Рис. 281 – Сообщение системы об успешном удалении

Примечание. При нескольких одновременно выделенных объектах происходит их одновременное удаление и зачистка как группы. При этом появится окно подтверждения удаления с количеством зачищаемых объектов.

8.2 Очистка остаточной информации на объектах ВИ

Затирание производится записью маскирующей последовательности поверх освобождаемого пространства. Параметру «Количество циклов затирания» можно задать значение от одного до четырех циклов затирания. Чем большее число циклов затирания выбрано, тем надежнее происходит удаление информации. При этом следует учесть, что чем больше циклов затирания будет выбрано, тем больше времени эта процедура будет занимать.

8.2.1 Очистка остаточной информации из консоли на клиентах vSphere

Чтобы воспользоваться данной функцией необходимо на уровне группы vSphere в основном меню открыть вкладку «Параметры безопасности vSphere» и нажать кнопку «Очистка остаточной информации». В рабочей области появится параметр «[Гипервизоры] Количество циклов затирания». Данному параметру можно установить значение от одного до четырех циклов затирания. Чтобы изменить это количество, необходимо произвести двойной клик по указанному параметру и в открывшемся окне выставить нужное значение (рис. 282). Затем нажать кнопку «Применить» и в категории «Действия» нажать кнопку «Сохранить».

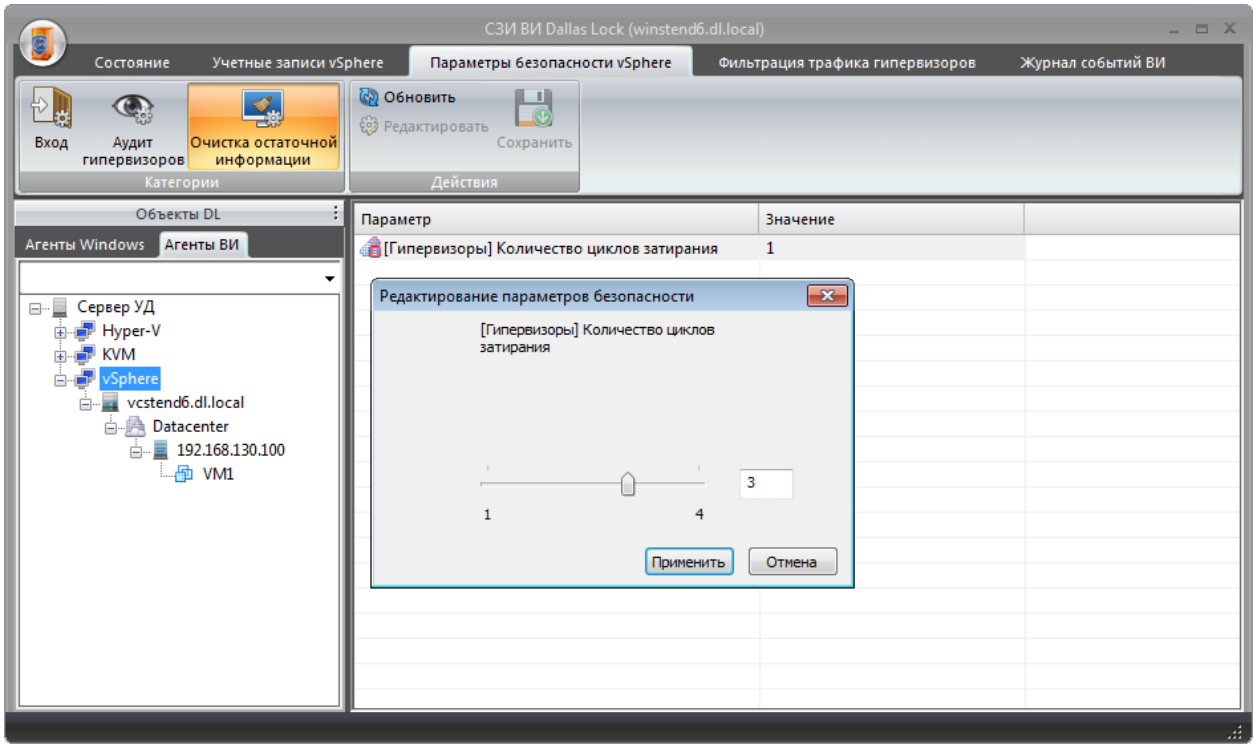


Рис. 282 – Установка количества циклов затирания

На уровне СВ и гипервизора также можно задать значение данного параметра на вкладке «Параметры безопасности vSphere». Кроме того, в окне редактирования параметров безопасности можно опционально установить флаг в поле «Наследуется» (рис. 283), тогда настройки параметра «[Гипервизоры] Количество циклов затирания» будут аналогичны настройкам, установленным на уровень выше.

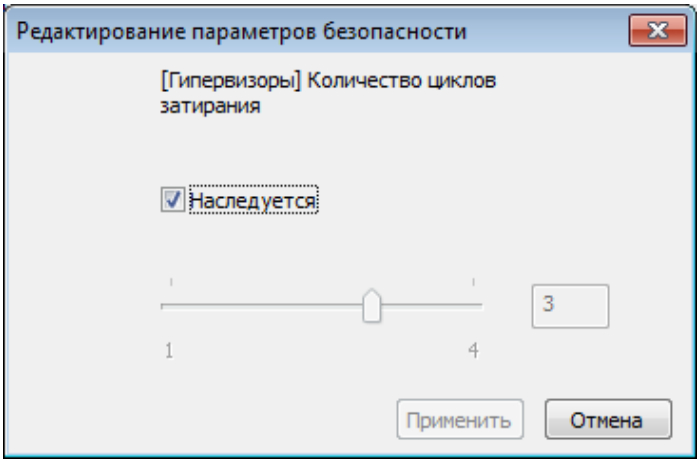


Рис. 283 – Наследование значения параметра «Количество циклов затирания»

Для зачистки ВМ необходимо:

1. Перейти на уровень удаляемой ВМ и во вкладке «Состояние» в блоке «Действия» нажать кнопку «Удалить и зачистить».
2. В появившемся диалоговом окне подтвердить удаление ВМ.

8.2.2 Очистка остаточной информации из консоли на гипервизорах KVM/oVirt/zVirt/HOSTVM/РЕД Вирт

Чтобы воспользоваться данной функцией необходимо на уровне группы KVM или на уровне СВ KVM/oVirt/zVirt/HOSTVM/РЕД Вирт (для индивидуальной настройки) в основном меню открыть вкладку «Параметры безопасности KVM» и нажать кнопку «Очистка остаточной информации». В рабочей области появится параметр «Количество циклов затирания». Данному параметру можно установить значение от одного до четырех циклов затирания. Чтобы изменить это количество, необходимо произвести двойной клик по указанному параметру и в открывшемся окне выставить нужное значение (рис. 284). Затем нажать кнопку «Применить» и в категории «Действия» нажать кнопку «Сохранить».

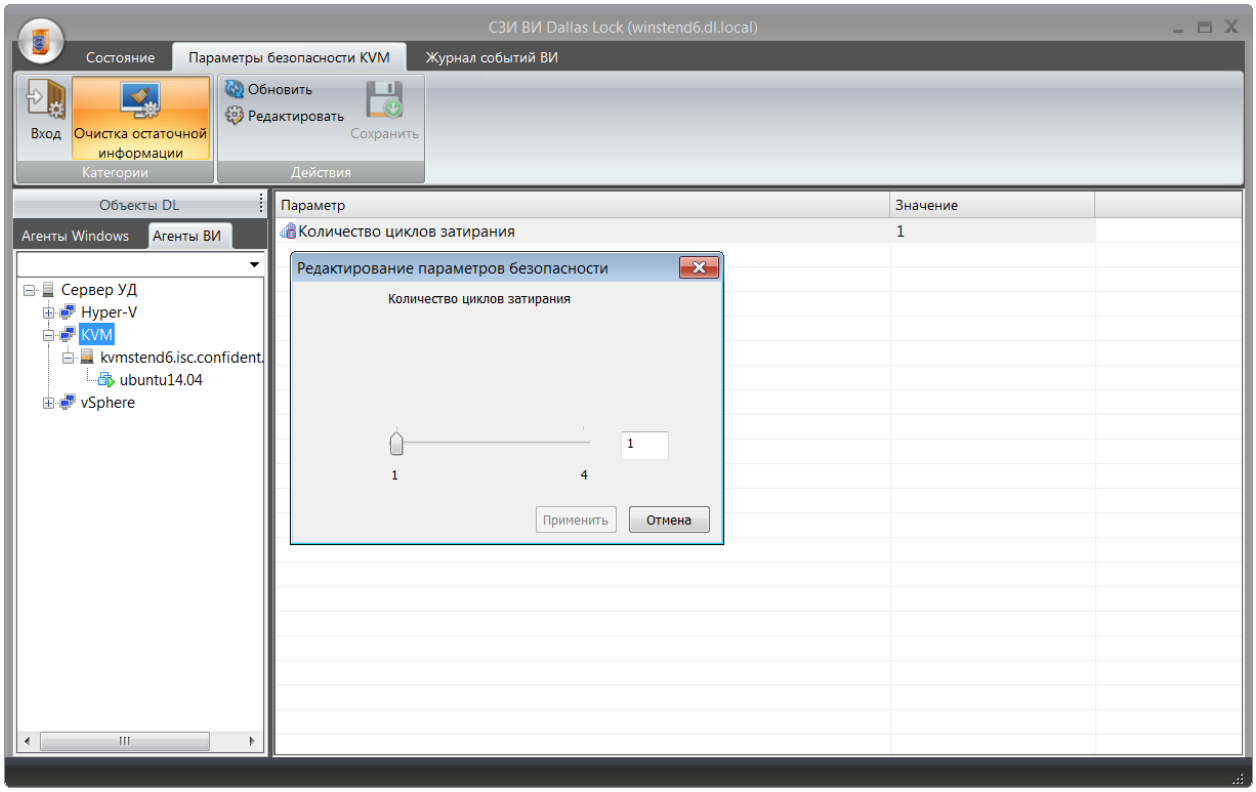


Рис. 284 – Установка количества циклов затирания для KVM

8.2.3 Удаление и зачистка виртуальной машины

Чтобы удалить и зачистить виртуальную машину, необходимо перейти в дерево «Агенты ВИ», выбрать виртуальную машину, выбрать категорию «Основное» → «Действия» → «Удалить и зачистить». После этого появится окно, уведомляющее о ходе процесса удаления и зачистки (рис. 285).

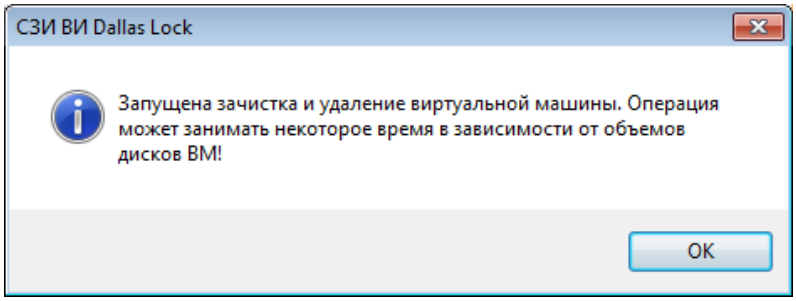


Рис. 285 – Удаление и зачистка виртуальной машины

Примечание. Процедура зачистки может занимать продолжительное время при объеме данных более 100GB.

Внимание! В случае, если происходит блокировка операции «Удалить и зачистить» ВМ Hyper-V для пользователя с форматом имени «<домен>\<имя_СВ>$», то необходимо:

1. В дереве «Агенты ВИ» на уровне Hyper-V выбрать категорию «Клиенты управления СВ», нажать кнопку «Добавить клиента» в блоке «Действия с клиентами».
2. Указать имя клиента, в формате «<домен>\<имя_СВ>» (символ «$» не прописывается).
3. В появившемся диалоговом окне необходимо подтвердить продолжение операции, нажав кнопку «Да».
4. Нажать кнопку «Синхронизировать» в блоке «Действия с Hyper-V».
5. Дождаться окончания процедуры синхронизации и повторить операцию «Удалить и зачистить».

8.2.4 Очистка информации с помощью утилиты Eraser

Во время установки агента DL ESXi на гипервизор дополнительно устанавливается утилита Eraser.

Eraser – это утилита для зачистки конфигурации и образов дисков виртуальных машин, которая гарантирует предотвращение восстановления удаленных данных.

Для работы с утилитой необходимо получить доступ к интерфейсу командной строки гипервизора. Для этого существует несколько способов:

- локальная командная строка, доступная с локальной консоли гипервизора при нажатии комбинации клавиш «Alt+F1»;
- подключение через SSH;
- подключение через vSphere PowerCLI.

Примечание. Данная утилита работает с именами, не содержащими кириллические символы.

Получив доступ к командной строке гипервизора, необходимо авторизоваться с правами администратора. Для работы с утилитой Eraser доступны следующие команды.

eraser -bN
Позволяет задать размер буфера для обработки больших файлов. По умолчанию значение 64Кб.
eraser -h
Позволяет вызвать справку с описанием утилиты и возможных ключей.
eraser -i
Позволяет продолжить процесс удаления, если встретились ошибки (права доступа и т.д.).
eraser -nN
Позволяет изменить количество проходов перезаписи, где N количество проходов от 1 до 35. По умолчанию значение 3.
eraser -r
Позволяет удалить каталог и все вложенные в него объекты.
eraser -v
Позволяет показать общую информацию о процессе удаления. Возможно использовать ключ -v дважды [-vv] для отображения прогресса удаления каждого файла.

8.2.4.1 Пример зачистки ВМ

Рассмотрим пример зачистки ВМ используя локальную командную строку гипервизора. Для этого необходимо:

1. Получить доступ к локальной командной строке гипервизора используя комбинацию клавиш «Alt+F1».
2. Ввести логин и пароль администратора гипервизора (рис. 286).

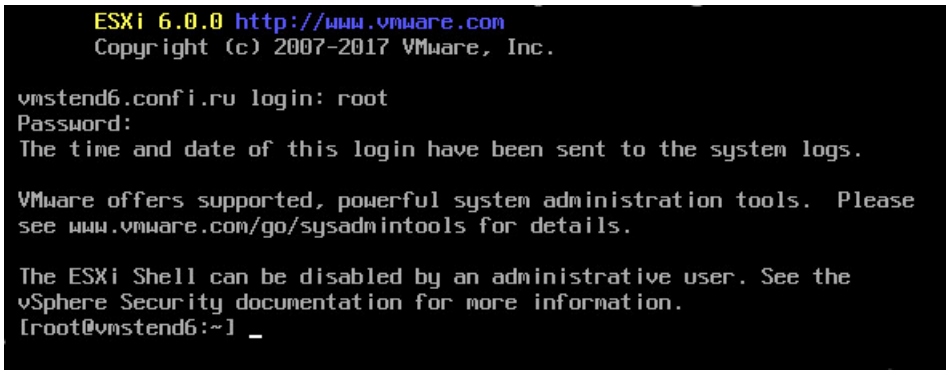


Рис. 286 - Ввод логина и пароля администратора гипервизора

3. Перейти в каталог с виртуальными машинами используя команду "cd *путь к каталогу*" (рис. 287). Для отображения объектов ФС в текущем каталоге возможно ввести команду "ls –la".

Примечание. Утилита Eraser работает глобально из любого каталога, но рекомендуется перед удалением перейти в нужный каталог. Это позволит избежать ошибочной зачистки, т.к. после нее восстановление данных невозможно.

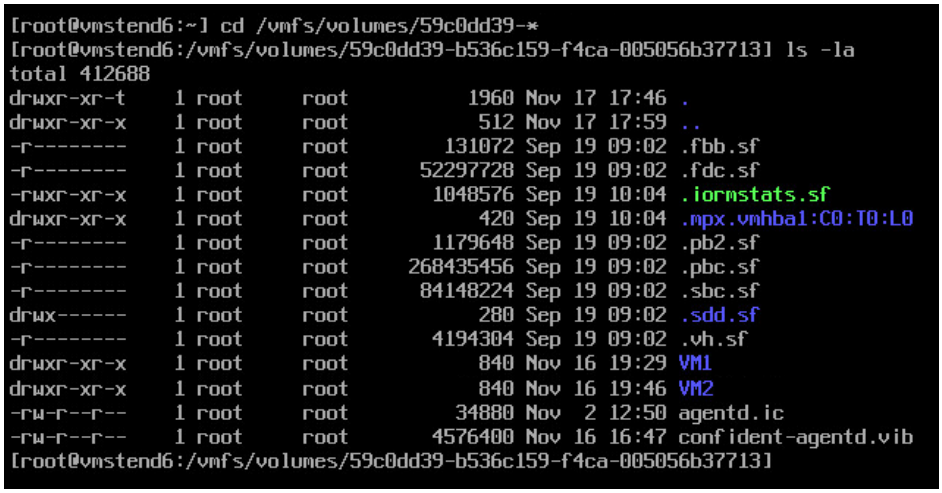


Рис. 287 - Переход в каталог

4. Выполнить команду "eraser –n4 –v –r *Имя каталога с ВМ*" и дождаться зачистки (рис. 288).

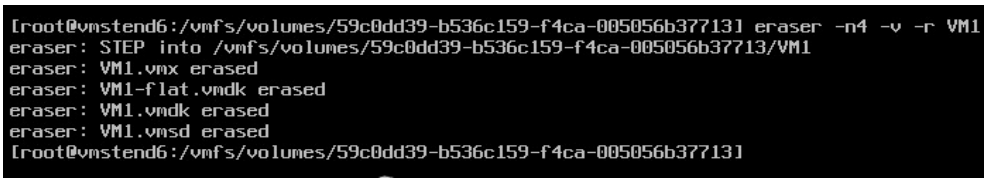


Рис. 288 - Зачистка ВМ

Примечание. Необходимо соблюдать регистр (нижний или верхний) при вводе команды, иначе она не будет выполнена.

9 ПОДСИСТЕМА АУДИТА

9.1 Аудит гипервизоров

9.1.1 Аудит гипервизоров ESXi

События безопасности регистрируются на всех гипервизорах, на которых установлен агент, после чего пересылаются на ЦУ СЗИ ВИ.

Просмотр и редактирование параметров аудита гипервизоров для гипервизоров vSphere происходит на уровне «vSphere» в категории «Параметры безопасности vSphere» → «Аудит гипервизоров» (рис. 289).

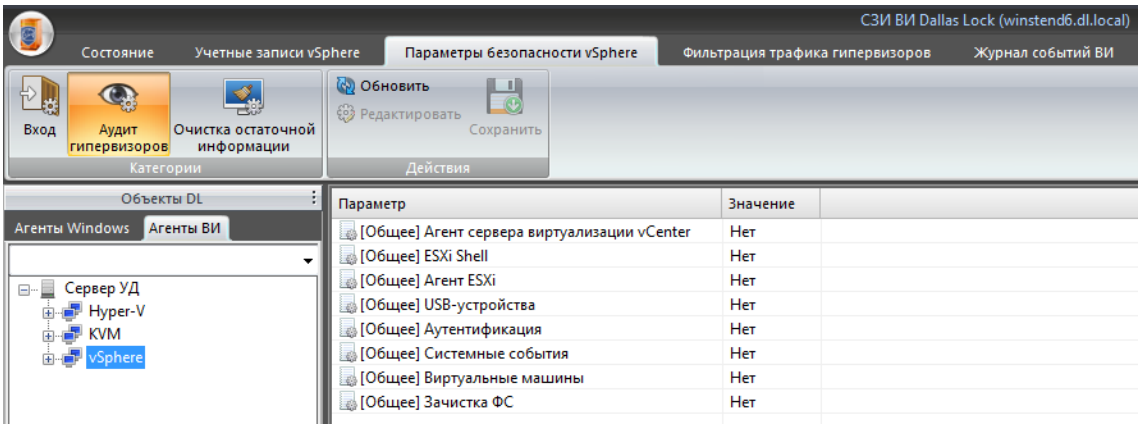


Рис. 289 – Аудит гипервизоров

В соответствии с настроенными параметрами информация регистрируется в журнале гипервизора (см. п. 9.1.7 «Журнал гипервизора (ESXi)»).

Доступны следующие параметры:

[Общее] Агент сервера виртуализации vCenter
Данный параметр позволяет включить регистрацию сведений о действиях агента, который взаимодействует с сервером виртуализации.
[Общее] ESXi Shell
Данный параметр позволяет включить регистрацию событий и записей всех введенных команд в ESXi Shell.
[Общее] Агент ESXi
Данный параметр позволяет включить регистрацию сведений о действиях агента, который управляет и конфигурирует гипервизор виртуальные машины, а также включить регистрацию событий аутентификации на гипервизоре.
[Общее] USB-устройства
Данный параметр позволяет включить регистрацию событий, связанных с подключаемыми USB-устройствами к гипервизору.
[Общее] Аутентификация
Данный параметр позволяет включить регистрацию событий, связанных с аутентификацией на гипервизоре.
[Общее] Системные события
Данный параметр позволяет включить регистрацию общих сообщений журнала (Syslog), которые могут быть использованы для устранения неполадок.
[Общее] Виртуальные машины
Данный параметр позволяет включить регистрацию событий, связанных с виртуальными машинами и гипервизорами.
[Общее] Зачистка ФС
Данный параметр позволяет включить регистрацию событий, связанных с зачисткой файловой системы гипервизора.

9.1.2 Аудит гипервизоров Hyper-V

Просмотр и редактирование параметров аудита гипервизоров для гипервизоров Hyper-V происходит на уровне группы Hyper-V в категории «Параметры безопасности Hyper-V» → «Аудит гипервизоров» (рис. 290).

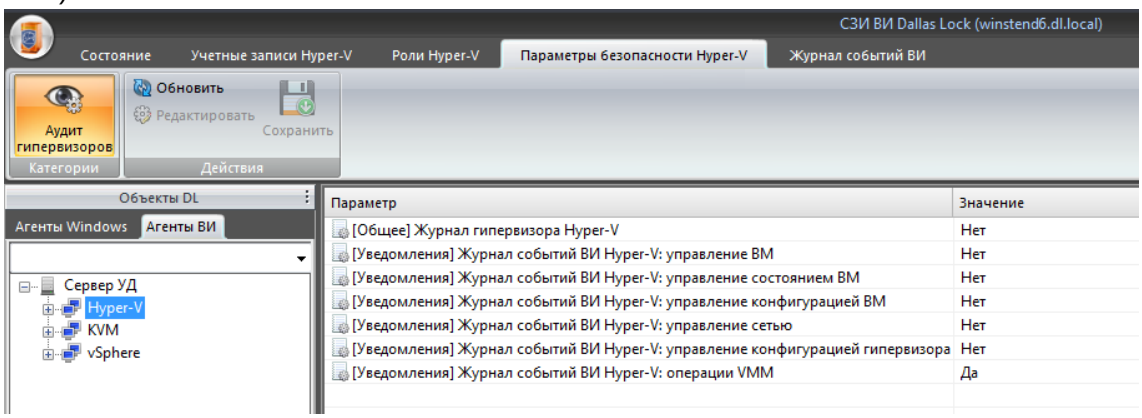


Рис. 290 – Аудит гипервизоров Hyper-V

Доступны следующие параметры:

[Общее] Журнал гипервизора Hyper-V
Данный параметр позволяет включить регистрацию событий, происходящих на гипервизоре Hyper-V. Параметр может принимать значение «Да» или «Нет».
[Уведомления] Журнал событий ВИ Hyper-V: управление ВМ
Данный параметр позволяет включить регистрацию событий, связанных с управлением ВМ. Параметр может принимать значение «Да» или «Нет».
[Уведомления] Журнал событий ВИ Hyper-V: управление состоянием ВМ
Данный параметр позволяет включить регистрацию событий, связанных с управлением состоянием ВМ. Параметр может принимать значение «Да» или «Нет».
[Уведомления] Журнал событий ВИ Hyper-V: управление конфигурацией ВМ
Данный параметр позволяет включить регистрацию событий, связанных с конфигурацией ВМ. Параметр может принимать значение «Да» или «Нет».
[Уведомления] Журнал событий ВИ Hyper-V: управление сетью
Данный параметр позволяет включить регистрацию событий, связанных с управлением сетью. Параметр может принимать значение «Да» или «Нет».
[Уведомления] Журнал событий ВИ Hyper-V: управление конфигурацией гипервизора
Данный параметр позволяет включить регистрацию событий, связанных с управлением конфигурацией гипервизора. Параметр может принимать значение «Да» или «Нет».
[Уведомления] Журнал событий ВИ Hyper-V: операции VMM
Данный параметр позволяет включить регистрацию событий, связанных с управлением хостами, кластерами и облачным сервисом.
[VMM] Блокировать SC VMM
Данный параметр позволяет заблокировать возможность подключения к серверу **VMM**. По умолчанию значение данного параметра: «Нет». **Примечание**. Данная политика доступна только на уровне сервера VMM в дереве объектов ВИ.

Чтобы изменить значение параметра, необходимо выбрать этот параметр в списке и вызвать окно редактирования параметров безопасности двойным щелчком мыши либо нажав кнопку

«Редактировать» в блоке «Действия». Выбрать значение и нажать кнопку «ОК» (рис. 291).

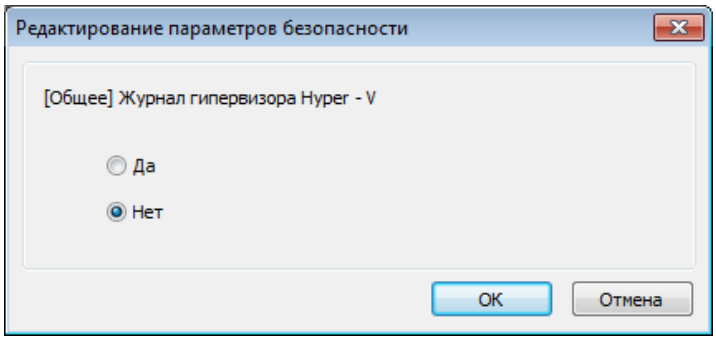


Рис. 291 – Редактирование параметров аудита гипервизоров Hyper-V

После внесения всех изменений необходимо в блоке «Действия» нажать кнопку «Сохранить».

Параметры, настроенные на уровне группы Hyper-V, по умолчанию наследуются на уровне серверов виртуализации (подробнее см. п. 3.8 «Наследование настроек»).

Для редактирования параметров наследования необходимо перейти на уровень сервера виртуализации Hyper-V на вкладку «Параметры безопасности Hyper-V» и выбрать категорию «Аудит гипервизоров» (рис. 292).

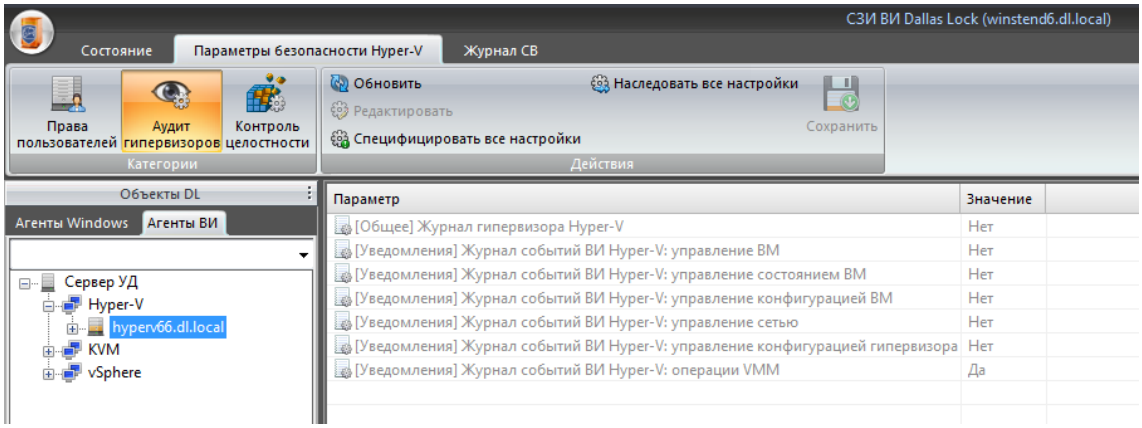


Рис. 292 – Настройка параметров аудита гипервизоров Hyper-V

Чтобы отменить наследование всех настроек параметров аудита гипервизоров группы Hyper-V в блоке «Действия» необходимо нажать кнопку «Специфицировать все настройки». Чтобы включить наследование всех настроек параметров аудита гипервизоров группы Hyper-V в блоке «Действия» необходимо нажать кнопку «Наследовать все настройки».

Для настройки конкретного параметра необходимо двойным щелчком мыши на нем либо нажатием кнопки «Редактировать» в блоке «Действия» вызвать окно редактирования параметров безопасности. Выбрать необходимое значение и нажать кнопку «ОК» (рис. 293).

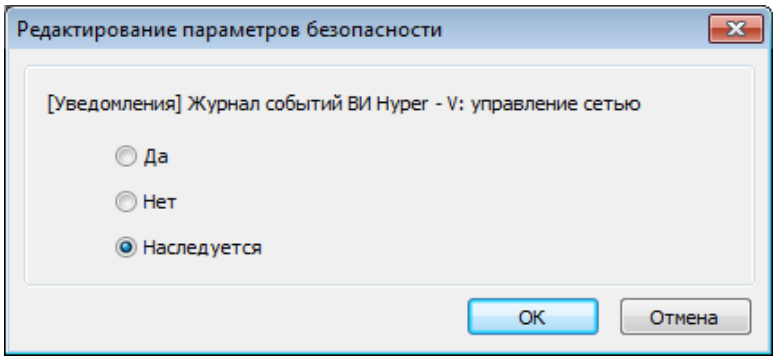


Рис. 293 – Редактирование параметров аудита гипервизоров Hyper-V на уровне СВ

После внесения всех изменений необходимо в блоке «Действия» нажать кнопку «Сохранить».

9.1.3 Журналы событий

В ЦУ СЗИ ВИ регистрируются события и группируются, в зависимости от типов событий, подлежащих протоколированию, также задается степень детализации аудита и другие факторы. Для этого используются следующие журналы:

1. Журнал ЦУ СЗИ ВИ.
2. Журнал событий ВИ (для каждой из групп vSphere, Hyper-V, KVM).

3. Журнал сервера виртуализации (для каждого СВ vSphere, Hyper-V, KVM).
4. Журнал гипервизора (только для ESXi).
5. Журнал событий oVirt/zVirt/HOSTVM/РЕД Вирт (только для СВ oVirt/zVirt/HOSTVM/РЕД Вирт).
6. Системный журнал (только для СВ oVirt/zVirt/HOSTVM и гипервизоров KVM и oVirt/zVirt/HOSTVM/РЕД Вирт).

В каждом журнале фиксируются дата, время, событие, результат и прочие параметры. Возможно упорядочивание элементов списков журнала по необходимому значению, для этого нужно кликнуть на кнопку с названием столбца журнала.

Двойной щелчок мышки на любой записи любого журнала открывает окно, содержащее всю информацию, относящуюся к этой записи (рис. 294).

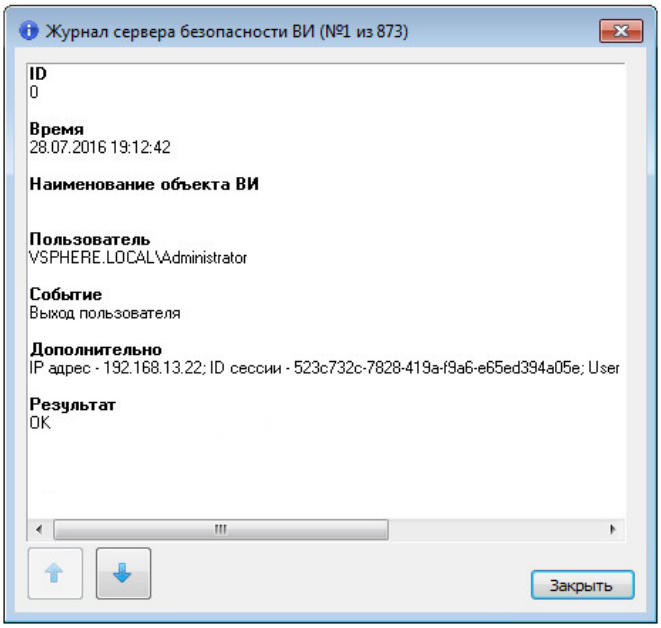


Рис. 294 – Отдельная форма записи журнала событий

Нажимая на кнопки «вверх» и «вниз», можно листать журнал, просматривая предыдущие или следующие записи.

Каждый текущий журнал формируется в папке «C:\DLVI\Jrn».

На панели «Действия» расположены элементы управления журналом. При нажатии кнопки «Обновить» отображаемые данные журналов после применения к ним новых настроек будут обновлены. Чтобы собрать информацию, отображенную в журналах, нужно нажать кнопку «Архивировать». После выбора архивации журнала, его записи сохраняются в файл в системной папке «C:\DLVI\Logs», в окне журнала записи очищаются, и он начинает вестись заново. Также, в случае, когда журнал переполняется (максимальный размер – 20000 записей), он архивируется в файл со специальным расширением *.lg8 и помещается в папку «C:\DLVI\Logs». При этом текущий журнал очищается и начинает вестись заново. В имени архивного файла с журналом записаны его тип, дата и время создания файла. Для открытия такого файла, необходимо нажать кнопку «Открыть из файла», а затем, в открывшемся окне, выбрать файл журнала или задать путь к файлу. Чтобы вернуться к просмотру текущего журнала, можно перейти на любую другую вкладку и вновь перейти к журналу. Кнопка «Экспорт» отвечает за сбор и конвертирование информации журналов в файлы с расширением txt (с табуляцией или без), CSV, HTML или XML. Для осуществления данной функции нужно нажать кнопку «Экспорт», указать имя файла и выбрать место для его хранения.

Примечание. При открытии «Открытие из файла», в окне выбора файлов возможно выбрать несколько журналов одного типа. При выборе разных типов появится сообщение об ошибке.

Для полного удаления журнала, необходимо открыть папку «C:\DLVI\Logs» и удалить соответствующий файл.

9.1.4 Журнал ЦУ СЗИ ВИ

Журнал ЦУ СЗИ ВИ – это журнал, в который заносятся события, связанные непосредственно с работой ЦУ СЗИ ВИ. Регистрируются такие события, например, как:

- Запуск или остановка службы ViCoreService.exe;

- Добавление или удаление сервера виртуализации;
- Запуск, приостановка или остановка виртуальной машины;
- Сбор журнала с сервера виртуализации;
- Начало или окончание периодического сбора журналов;
- Начало или окончание сбора журналов с серверов Hyper-V;
- Начало или окончание периодического сбора журналов;
- Начало или окончание сбора журналов с серверов vCenter;
- Неверно указано имя пользователя или пароль;
- Доступ пользователю запрещен;
- Нет доступа для соединения с гипервизором;
- Отсутствует файл конфигурации виртуальной машины;
- Ошибка при запуске виртуальной машины;
- Попытка запуска виртуальной машины с нарушенной целостностью файлов;
- Установка или снятие нотификации с агента;
- Контроль состояния агента;
- Архивация журнала событий ВИ.
- Архивация журналов ЦУ СЗИ ВИ, ВИ, гипервизора.
- Обновление сертификатов на агенте.
- Вход пользователя VMware.
- Перезапуск или удаление виртуальной машины.
- Удаление и зачистка виртуальной машины.
- События на уровне vSphere;
- Общая ошибка системы.

Также в журнал ЦУ СЗИ ВИ заносятся типы событий, при которых происходит событие сигнализации (воспроизводится звуковой сигнал и выводится сообщение):

- Нарушение контроля целостности файлов виртуальных машин.
- Нарушение контроля целостности системных файлов и конфигураций хоста.
- Попытка запуска виртуальной машины с нарушенным контролем целостности.
- Попытка получения доступа при наличии ограничений из-за разрешений сервера виртуализации (через анализ собранных журналов).

Просмотр журнала происходит на уровне «Сервер УД» на вкладке «Журнал ЦУ СЗИ ВИ» (рис. 295).

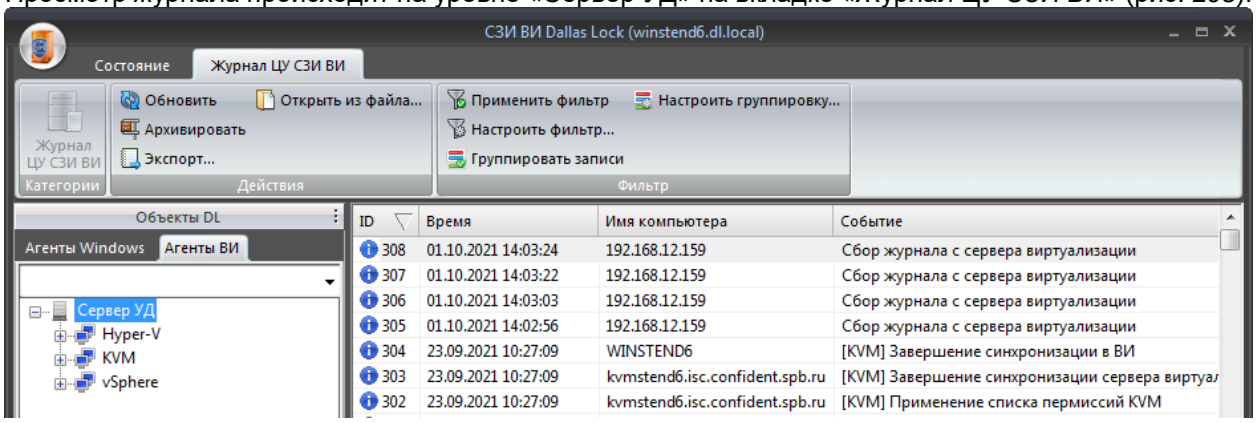


Рис. 295 – Журнал ЦУ СЗИ ВИ

Управление журналом описано в п. 9.1.3 «Журналы событий».
Управление фильтрацией журнала производится в категории «Фильтр». Для задания параметров фильтра необходимо нажать на кнопку «Настроить фильтр». В появившемся окне можно задать количество и тип записей, период времени, за который необходимо отобразить события, дополнительные параметры. Фильтр также можно инвертировать фильтр. После завершения настройки фильтра необходимо нажать кнопку «ОК». Затем, чтобы применить настроенный фильтр, необходимо нажать кнопку «Применить фильтр». Для отмены фильтрации следует нажать на ту же кнопку.
В категории «Фильтр» также можно настроить группировку записей журнала по полям. Чтобы применить настройки группировки необходимо нажать на кнопку «Группировать записи».

9.1.5 Журнал событий ВИ

Журнал событий ВИ – это журнал, который содержит информацию об операциях над контролируемыми объектами на Сервере виртуализации, поступающую от агентов DL. Для получения событий необходим настроенные параметры аудита (см. п. 9.1.1 «Аудит гипервизоров

ESXi» и 9.1.2 «Аудит гипервизоров Hyper-V»).

Просмотр журнала происходит на уровне групп Hyper-V, KVM либо vSphere на вкладке «Журнал событий ВИ» (рис. 296).

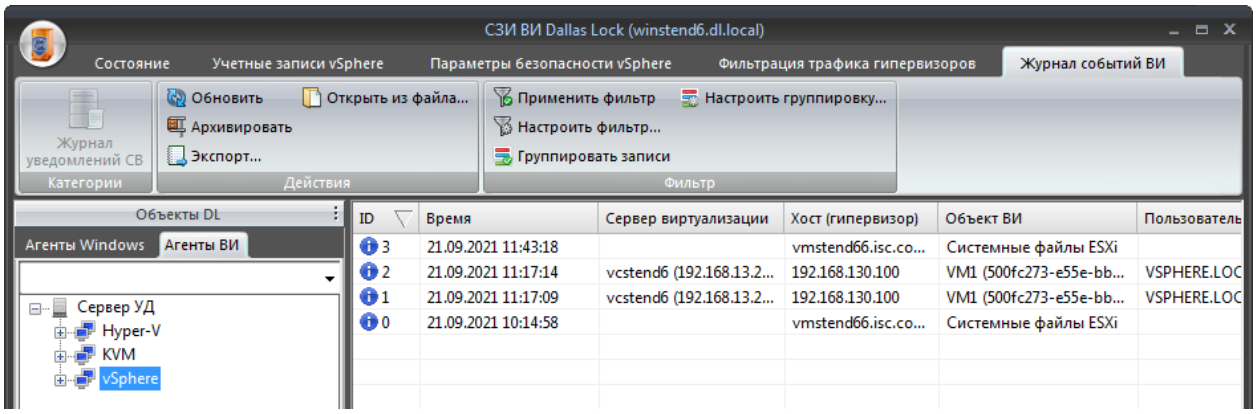


Рис. 296 – Журнал событий ВИ

Формирование этого журнала происходит в режиме реального времени. Управление журналом описано в п. 9.1.3 «Журналы событий».

Фильтрация осуществляется по аналогии с фильтрацией журнала ЦУ СЗИ ВИ и описана в п. 9.1.4 «Журнал ЦУ СЗИ ВИ».

9.1.6 Журнал сервера виртуализации

Журнал сервера виртуализации – это журнал, который содержит информацию об изменениях состояния управляемых объектов на сервере виртуализации. События включают в себя действия системы и пользователей, которые происходят на объектах ВИ.

Просмотр журнала СВ происходит на уровне Сервера виртуализации на вкладке «Журнал СВ» (рис. 297).

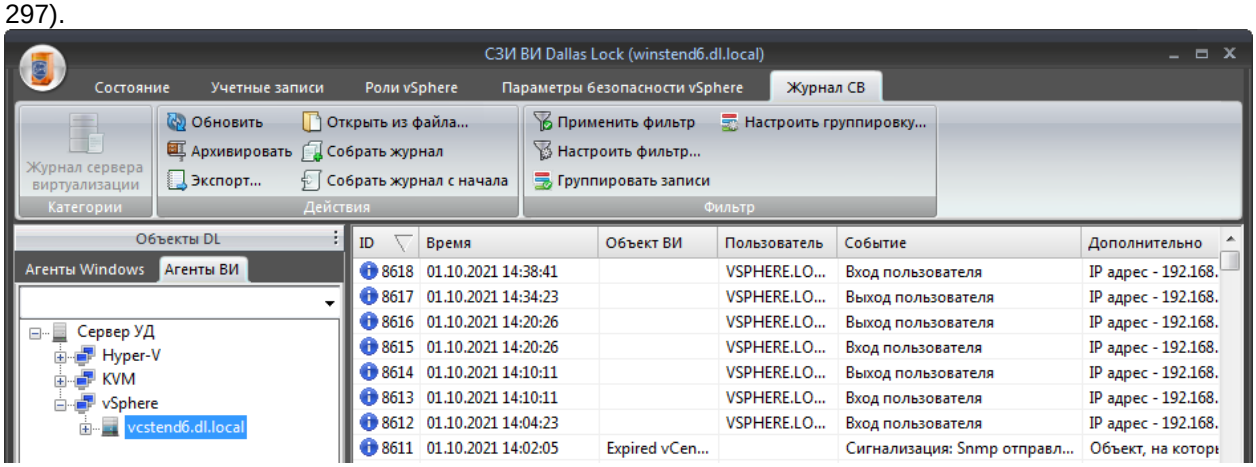


Рис. 297 – Журнал СВ

Формирование этого журнала происходит на момент команды сбора журнала путем нажатия кнопки «Собрать журнал», а также при настроенном периодическом сборе журналов в параметрах ЦУ СЗИ ВИ.

Примечание. В поле «Пользователь» журналов СВ vCenter/vCSA могут быть указаны в том числе и служебные пользователи VMware vCenter и VMware vCSA соответственно, даже если они не зарегистрированы в СЗИ ВИ.

Управление журналом описано в п. 9.1.3 «Журналы событий».

Фильтрация осуществляется по аналогии с фильтрацией журнала ЦУ СЗИ ВИ и описана в п. 9.1.4 «Журнал ЦУ СЗИ ВИ».

Для журналов серверов виртуализации возможно задать частоту и расписание периодического сбора журналов (см. п. 3.3 «Основные параметры»).

Просмотр и редактирование параметров сбора журналов СВ происходит в окне «Параметры сервера УД», которое вызывается выбором соответствующего пункта в дополнительном меню Консоли (подробнее см. п. 3.3 «Основные параметры»).

9.1.7 Журнал гипервизора (ESXi)

Журнал гипервизора – в данный журнал регистрируются события безопасности гипервизора, на котором установлен агент DL ESXi. Журнал включает в себя системные события и действия агента DL ESXi на гипервизоре. Для работы данного журнала должен быть настроен «Аудит гипервизора», например, для регистрации событий об аутентификации необходимо включить параметр «[Общее] Агент ESXi» (см. п. 9.1.1 «Аудит гипервизоров ESXi».

Просмотр журнала гипервизора происходит на уровне гипервизора на вкладке «Журнал гипервизора» (рис. 298).

Формирование этого журнала происходит в режиме реального времени. Для обновления информации необходимо нажать кнопку «Обновить».

Для удобства просмотра журнала возможно использовать поиск по словам.

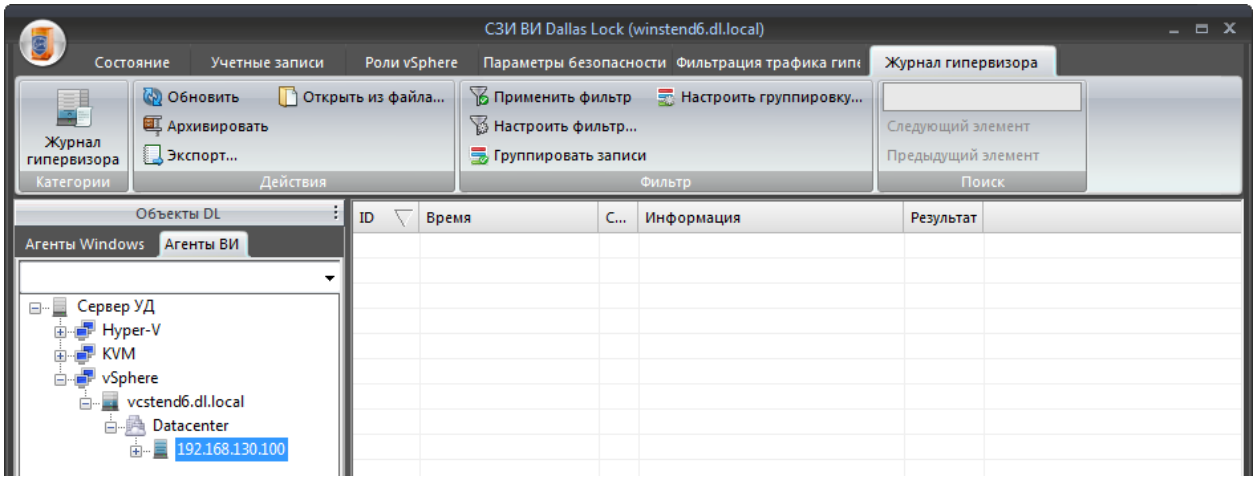


Рис. 298 – Журнал гипервизора

9.1.8 Журнал событий oVirt/zVirt/HOSTVM/РЕД Вирт

Журнал событий oVirt/zVirt/HOSTVM/РЕД Вирт – это журнал, который содержит информацию об изменениях состояния управляемых объектов на сервере виртуализации. События включают в себя действия системы и пользователей, которые происходят на объектах ВИ.

Просмотр журнала происходит на уровне Сервера виртуализации на вкладке «Журнал событий oVirt/zVirt/HOSTVM/РЕД Вирт» (рис. 299).

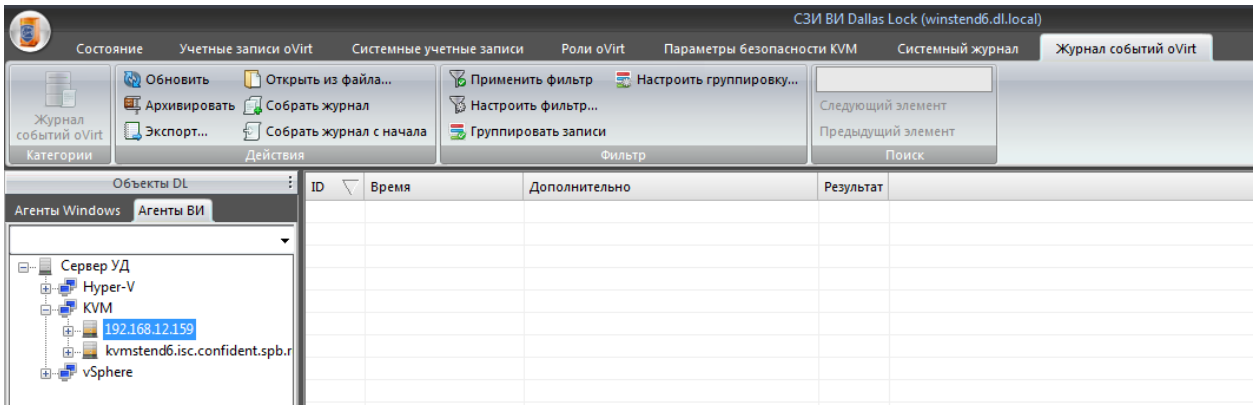


Рис. 299 – Журнал событий oVirt/zVirt/HOSTVM

Формирование этого журнала происходит на момент команды сбора журнала путем нажатия кнопки «Собрать журнал», а также при настроенном периодическом сборе журналов в параметрах ЦУ СЗИ ВИ.

Фильтрация осуществляется по аналогии с фильтрацией журнала ЦУ СЗИ ВИ и описана в п. 9.1.4 «Журнал ЦУ СЗИ ВИ».

9.1.9 Системный журнал (KVM/oVirt/zVirt/HOSTVM/РЕД Вирт)

Системный журнал – в данный журнал содержит события системного журнала ОС СВ oVirt/zVirt/HOSTVM/РЕД Вирт и гипервизоров KVM и oVirt/zVirt/HOSTVM/РЕД Вирт.

Просмотр журнала происходит на уровне сервера виртуализации/гипервизора на вкладке «Системный журнал» (рис. 300).

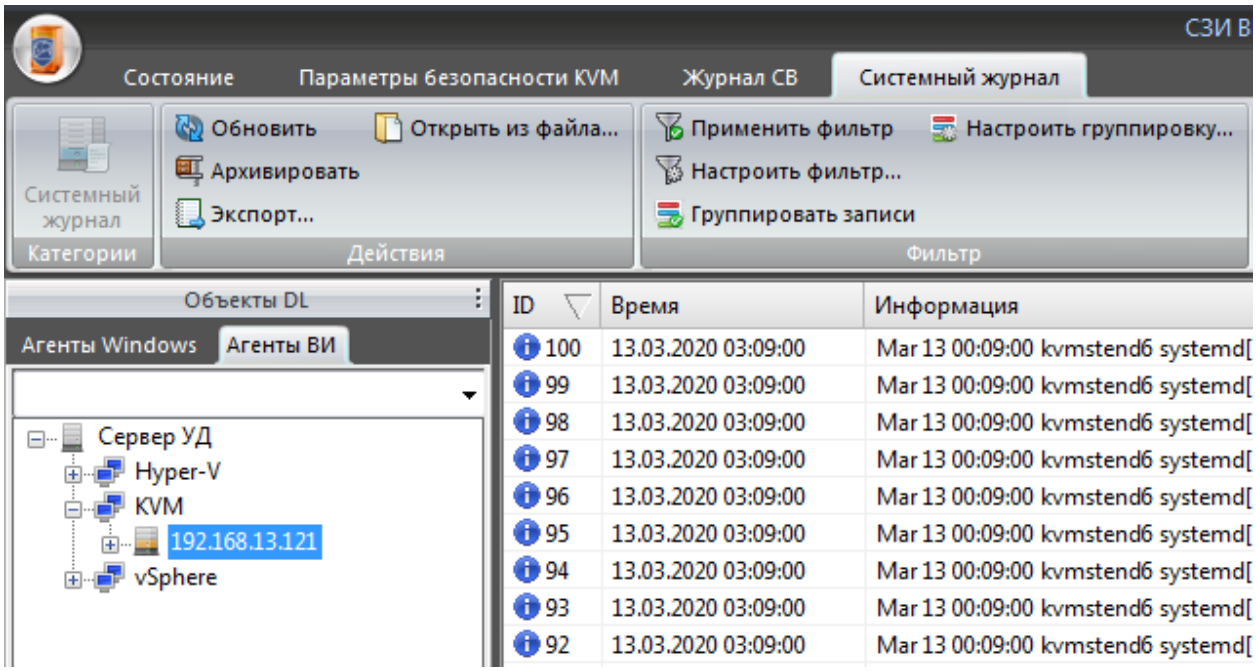


Рис. 300 – Системный журнал

Формирование этого журнала происходит в режиме реального времени. Для обновления информации необходимо нажать кнопку «Обновить».

Для удобства просмотра журнала возможно использовать поиск по словам.

9.2 Аудит компьютеров клиентов Windows

9.2.1 Аудит событий на компьютерах клиентов Windows

С помощью подсистемы аудита в СЗИ ВИ происходит регистрация событий на клиентах и их группировка, в зависимости от типов событий, подлежащих протоколированию, также задается степень детализации аудита и другие факторы.

Чтобы настроить параметры аудита необходимо в дереве «Агенты Windows» на уровне Сервера УД перейти в «Параметры безопасности домена» → «Аудит» (рис. 301).

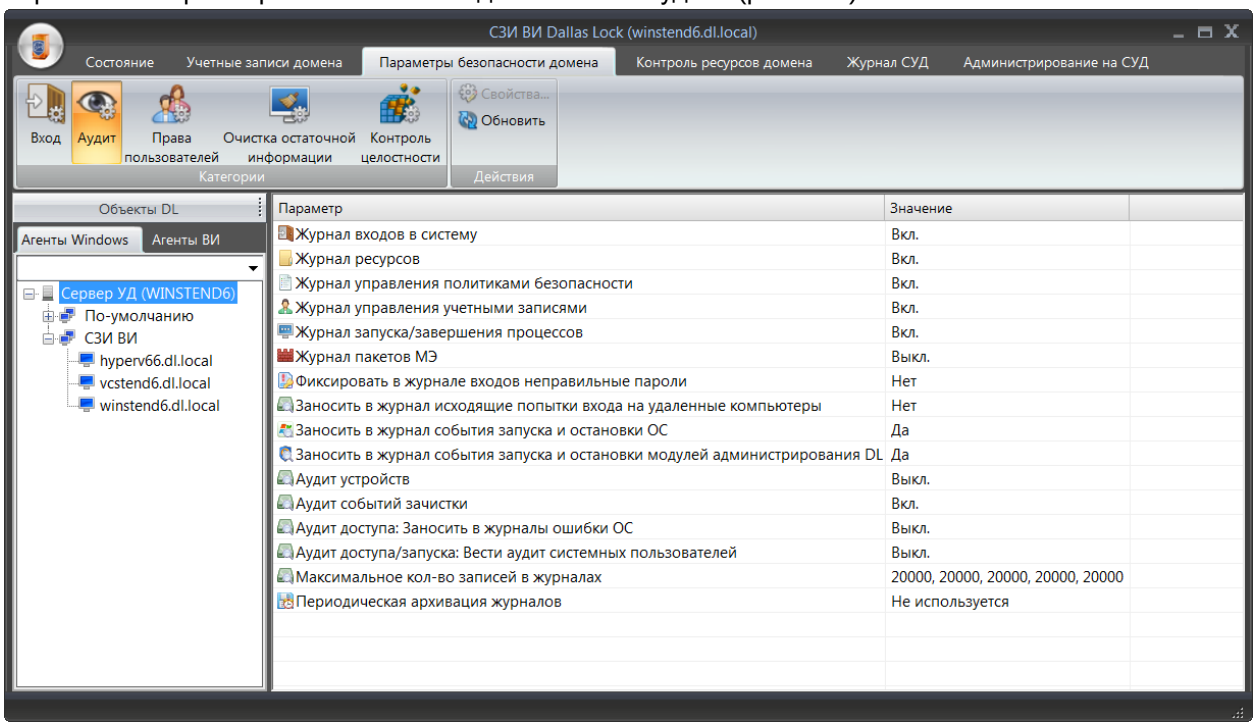


Рис. 301 – Аудит событий на компьютерах клиентов

Доступны следующие параметры:

Журнал входов в систему
Включение журнала позволяет протоколировать в нем события, связанные с входом, выходом, разблокировкой пользователей на ПК, включая как локальные, так и сетевые входы и выходы. Параметр может принимать значение «Вкл.» или «Выкл.».
Журнал ресурсов
Включение журнала позволяет протоколировать в нем события по доступу к ресурсам файловых систем, программно-аппаратной среды и к устройствам (при включенном параметре «Аудит устройств» – см. ниже). А также события очистки остаточной информации (при включении «Аудит событий зачистки»). Возможен аудит действий пользователей, как с локальными ресурсами, так и с сетевыми. Сюда же заносятся события непосредственно по управлению доступом к ресурсам (в случае, когда на объект назначается любой дескриптор доступа, аудита, контроля целостности). Параметр может принимать значение «Вкл.» или «Выкл.».
Журнал управления политиками безопасности
Включение журнала позволяет протоколировать в нем действия по настройке параметров системы защиты и по изменению прав пользователей. Параметр может принимать значение «Вкл.» или «Выкл.».
Журнал управления учетными записями
Включение журнала позволяет вести в нем учет действий по созданию, удалению, редактированию учетных записей пользователей. Параметр может принимать значение «Вкл.» или «Выкл.».
Журнал запуска/завершения процессов
Включение журнала позволяет протоколировать в нем события запусков/завершения процессов в ОС. Параметр может принимать значение «Вкл.» или «Выкл.».
Журнал пакетов МЭ
Включение журнала позволяет фиксировать все события, связанные с передачей пакетов данных в соответствии с заданными правилами в обоих направлениях через сетевые адаптеры компьютера. Параметр может принимать значение «Вкл.» или «Выкл.».
Фиксировать в журнале входов неправильные пароли
Включение данного параметра позволяет фиксировать значения неверно введенных паролей в журнале входов (при условии, что журнал входов включен). Параметр может принимать значение «Да» или «Нет». **Внимание!** При значении параметра «Да» возникает риск использования информации, содержащейся в столбце «Неверный пароль», для скрытой компрометации паролей пользователей. Ошибки пользователей при вводе пароля неминуемо приведут к раскрытию части пароля, что может значительно облегчить для злоумышленника задачу его подбора.
Заносить в журнал исходящие попытки входа на удаленные компьютеры
Включение данного параметра позволяет регистрировать события исходящей попытки входа пользователя на удаленный компьютер через ЛВС в журнале входов (при условии, что журнал входов включен). Параметр может принимать значение «Да» или «Нет».
Заносить в журнал события запуска и остановки ОС
Включение данного параметра позволяет регистрировать события, связанные с запуском/завершением работы ОС, события запуска/остановки ядра защиты СЗИ, в журнале управления политиками (при условии, что данный журнал включен). Параметр может принимать значение «Да» или «Нет».
Заносить в журнал события запуска и остановки модулей администрирования DL
Включение данного параметра позволяет регистрировать события, связанные с

запуском/завершением работы Консоли в журнале управления политиками (при условии, что данный журнал включен). Параметр может принимать значение «Да» или «Нет».

Аудит устройств

Включение данного параметра позволяет регистрировать события по доступу к подключаемым на данный ПК устройствам в Журнале ресурсов (при условии, что журнал ресурсов включен). Сами события настраиваются непосредственно в окне редактирования параметров дескриптора устройства (класса устройств).

Параметр может принимать значение «Вкл.» или «Выкл.».

Аудит событий зачистки

Включение данного параметра позволяет регистрировать события зачистки остаточной информации в следующих случаях:

- при включенных параметрах зачистки (см. «Очистка остаточной информации на объектах ВИ»);
- при зачистке по запросу пользователя (пункт контекстного меню «Удалить и зачистить», см. «Удаление файлов и зачистка остаточной информации по команде»).

Параметр может принимать значение «Вкл.» или «Выкл.».

Аудит доступа: Заносить в журналы ошибки ОС

Включение данного параметра позволяет вести учет ошибок доступа ОС Windows в журнале ресурсов (при условии, что журнал ресурсов включен). Так как СЗИ ВИ не подменяет механизмы контроля доступа к ресурсам операционной системы, а добавляет свои, то любое действие над файловой системой вначале попадает для проверки в драйвер защиты СЗИ ВИ, и, если этот драйвер разрешает данное действие, оно передается дальше ОС. Операционная система, в свою очередь, может отказать уже по своим причинам – эти отказы и протоколируются. В большинстве случаев аудит этих ошибок не требуется.

Параметр может принимать значение «Вкл.» или «Выкл.».

Аудит доступа/запуска: Вести аудит системных пользователей

Включение данного параметра позволяет вести учет действий системных пользователей (SYSTEM, LOCAL SERVICE, NETWORK SERVICE и пр.) в журнале ресурсов (при условии, что журнал ресурсов включен). В большинстве случаев, аудит этих пользователей не требуется.

Параметр может принимать значение «Вкл.» или «Выкл.».

Максимальное кол-во записей в журналах

Настройка данного параметра позволяет установить максимальное количество записей в следующих **журналах (рис. 302):**

- Журнал входов;
- Журнал упр. уч. записями;
- Журнал ресурсов;
- Журнал упр. политиками;
- Журнал процессов.

Параметр может принимать значение «Не используется» или числовое значение «100-20000».

Периодическая архивация журналов

Включение данного параметра позволяет управлять периодами автоматической архивации журналов. После настройки данного параметра, все журналы по расписанию архивируются, все записи из них сохраняются в файл в системной папке «C:\DLVI\Logs», записи журналов очищаются, и они начинают вестись заново.

По умолчанию параметру задано значение «Не используется». Границы возможного временного интервала архивации варьируются от 1 часа до 1 года.

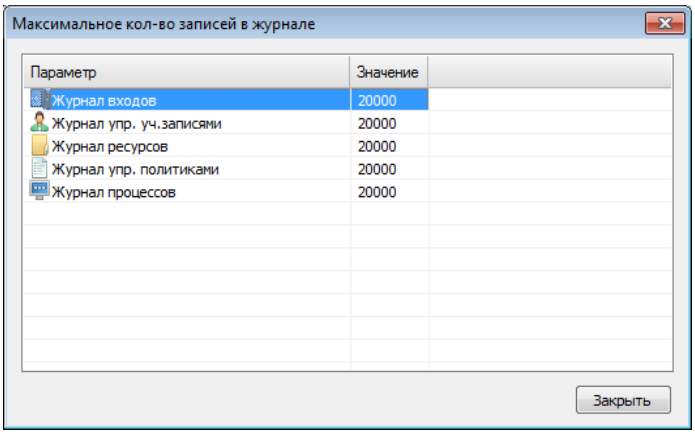


Рис. 302 – Максимальное количество записей в журналах

9.2.2 Журналы событий на компьютерах клиентов Windows

В ЦУ СЗИ ВИ регистрируются события и группируются, в зависимости от типов событий, подлежащих протоколированию, также задается степень детализации аудита и другие факторы. Для этого используются семь журналов (рис. 303):

1. Журнал сервера УД.
2. Журнал входов.
3. Журнал управления учетными записями.
4. Журнал ресурсов.
5. Журнал управления политиками.
6. Журнал процессов.
7. Журнал пакетов МЭ.

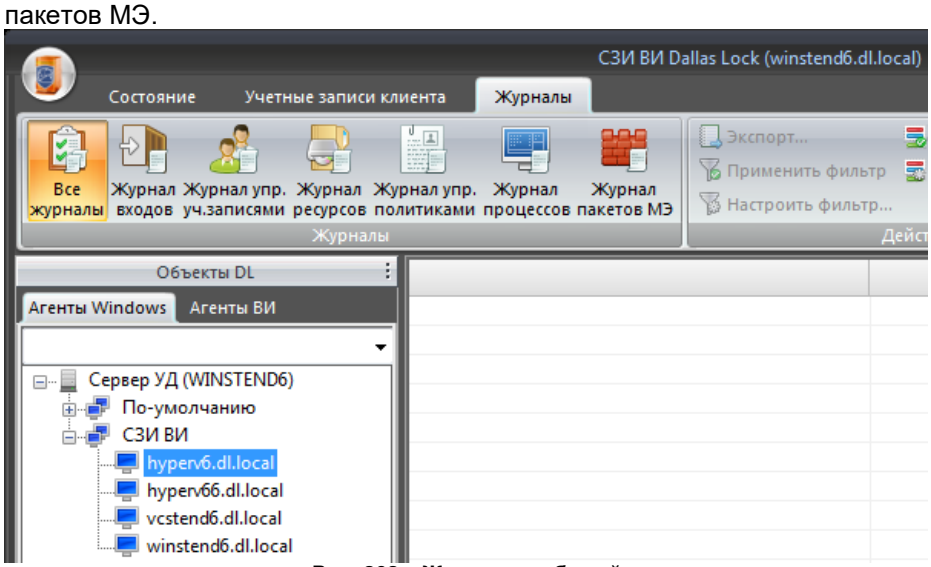


Рис. 303 – Журналы событий

В каждом журнале фиксируются дата, время, событие, результат и прочие параметры.

9.2.3 Журнал Сервера УД

Журнал Сервера УД (Журнал СУД) – это журнал, в который заносятся события, связанные непосредственно с работой подключенных клиентских компьютеров. Формирование этого журнала происходит в режиме реального времени.

Просмотр журнала Сервера УД происходит на уровне Сервера УД на вкладке «Журнал СУД» (рис. 304).

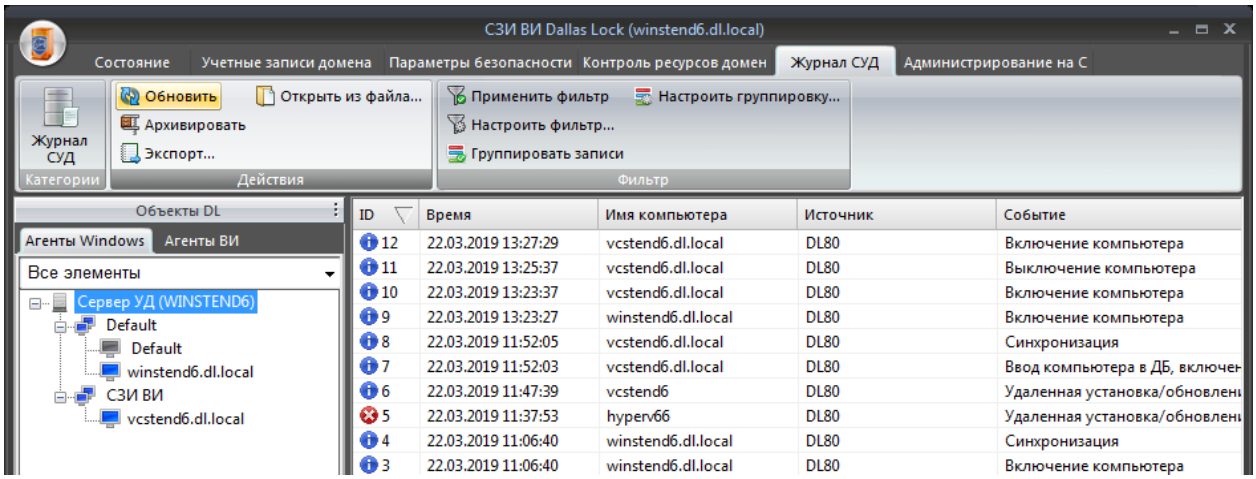


Рис. 304 – Журнал Сервера УД

9.2.4 Формирование журналов событий на компьютерах клиентов Windows

Формирование журналов осуществляется двумя способами:

1. Сбор журналов для всех клиентов.
2. Сбор журналов для выбранного клиента.

9.2.4.1 Сбор журналов для всех клиентов:

1. Перейти на уровень «Сервер УД» во вкладке «Агенты Windows».
2. В блоке «Действия с доменом» нажать кнопку «Собрать журналы» (рис. 305).

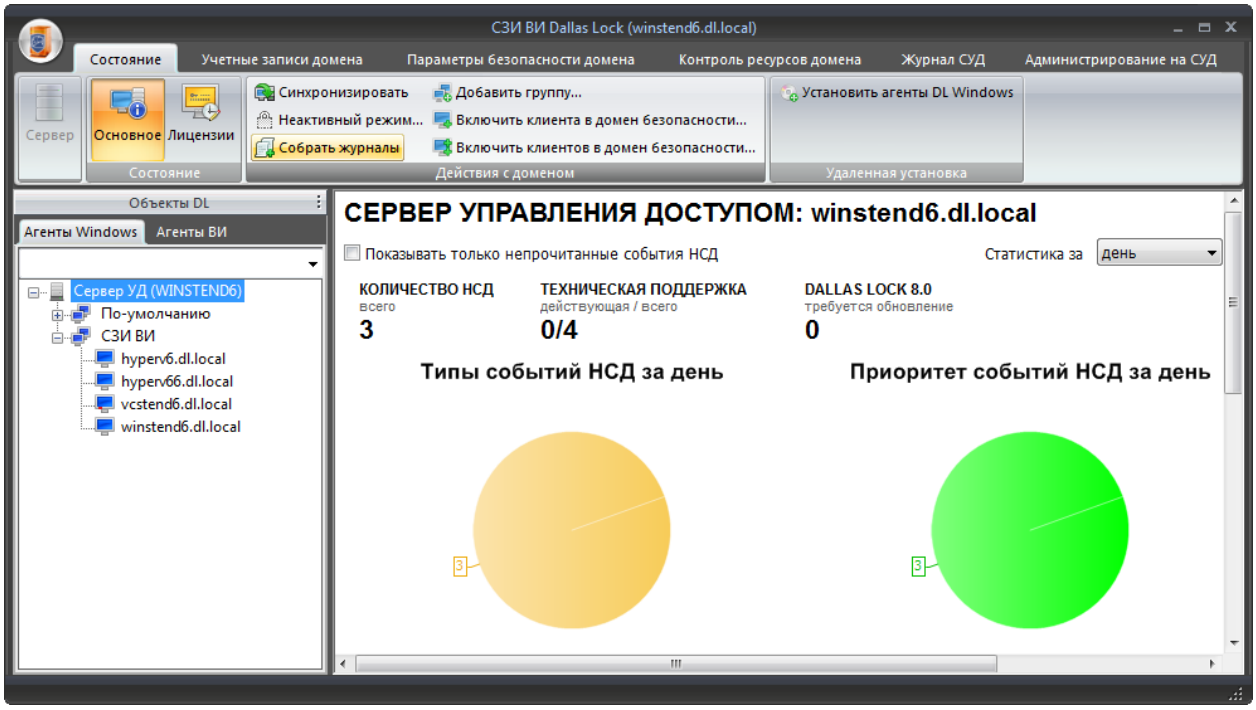


Рис. 305 – Сбор журналов событий

9.2.4.2 Сбор журналов для выбранного клиента:

1. Перейти на уровень клиента во вкладке «Агенты Windows».
2. Открыть вкладку «Журналы» и в категории «Действия с журналами» нажать кнопку «Собрать журналы» (рис. 306).

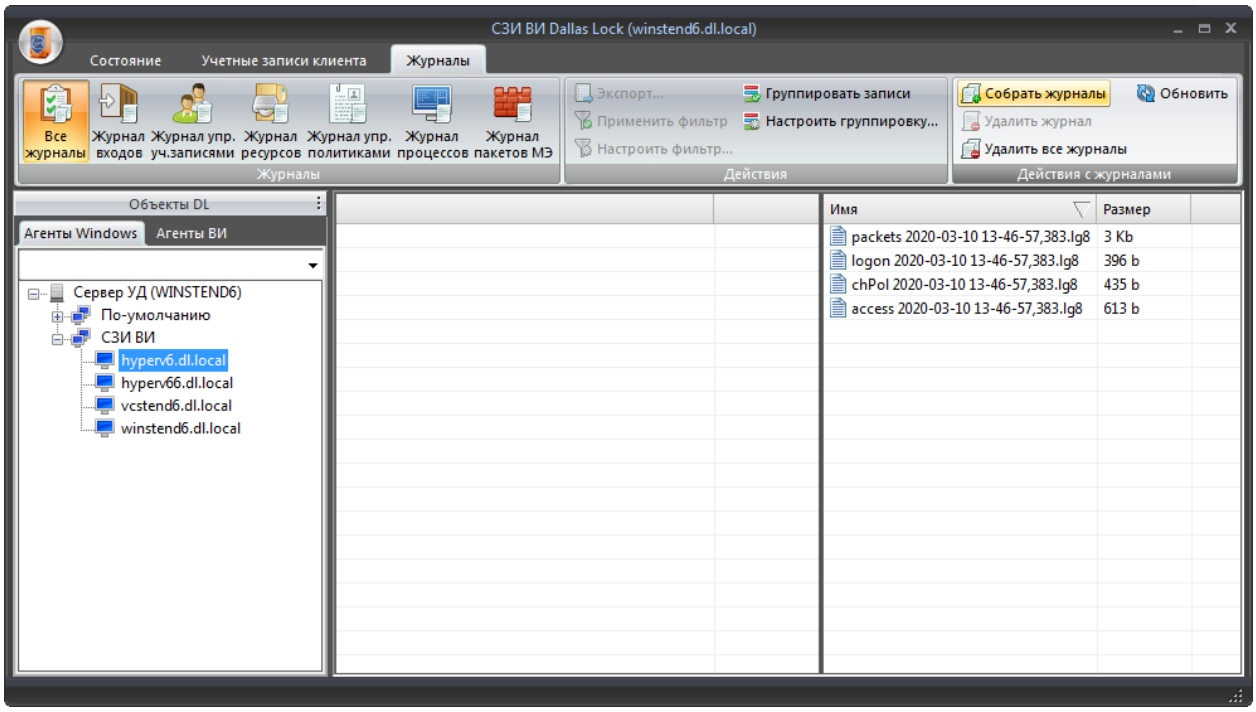


Рис. 306 – Сбор журналов для клиента

9.2.5 Просмотр журналов событий на компьютерах клиентов Windows

Просмотр журналов происходит на уровне клиента в дереве «Агенты Windows» во вкладке «Журналы» (рис. 307).

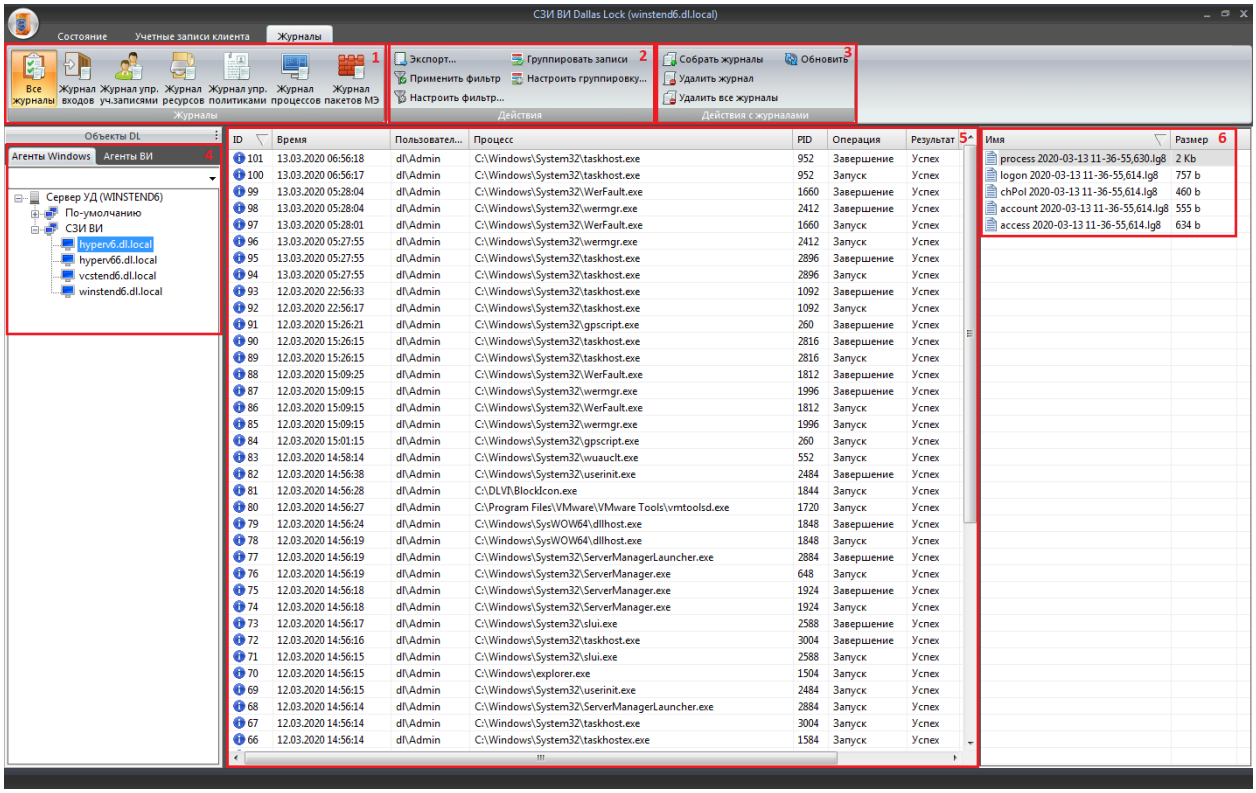


Рис. 307 – Вкладка «Журналы»

Вкладка «Журналы» содержит следующие рабочие области:

1. Категория «Журналы».
2. Категория «Действия».
3. Категория «Действия с журналами».
4. Дерево клиентов.
5. Список событий журнала.
6. Список сформированных журналов.

Для отображения списка событий необходимо выбрать журнал из списка и дождаться его открытия.

Возможно упорядочивание элементов списков журнала по нужному значению, для этого необходимо кликнуть на кнопку с названием столбца журнала.

В категории «Действия» расположены элементы управления записями журнала. Кнопка «Экспорт» отвечает за сбор и конвертирование информации журналов в файлы с расширением txt (с табуляцией или без), CSV, HTML или XML. Для осуществления данной функции нужно нажать кнопку «Экспорт», указать имя файла и выбрать место для его хранения. Для просмотра событий по различным критериям необходимо нажать кнопку «Настроить фильтр» и в открывшемся окне указать параметры отбора событий. Для применения выбранных критериев фильтрации необходимо нажать кнопку «Применить фильтр». Также можно группировать отображаемые записи по значению поля. Для этого необходимо воспользоваться кнопкой «Настроить группировку», отметить флагом необходимые поля. Кнопка «Группировать записи» отвечает за применение настроенной группировки.

Двойной щелчок мышки на любой записи любого журнала открывает окно, содержащее всю информацию, относящуюся к этой записи (рис. 308).

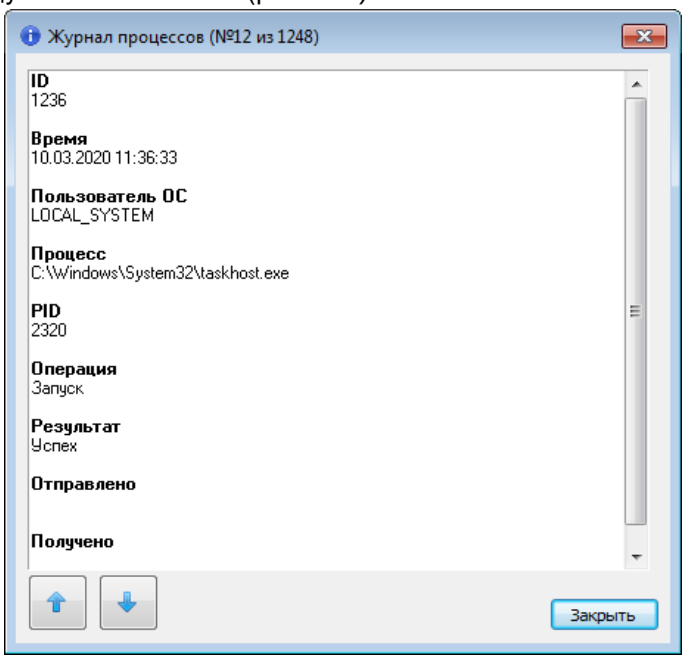


Рис. 308 – Отдельная форма записи журнала

Нажимая на кнопки «вверх» и «вниз», можно листать журнал, просматривая предыдущие или следующие записи.

Для удаления журнала, необходимо в категории «Действия с журналами» выбрать журнал и воспользоваться кнопкой «Удалить журнал». Также можно удалить все журналы, воспользовавшись кнопкой «Удалить все журналы».

10 ЕДИНЫЙ ЦЕНТР УПРАВЛЕНИЯ DALLAS LOCK

Для реализации централизованного управления различными модулями на клиентах необходимо использовать Единый центр управления Dallas Lock (ЕЦУ Dallas Lock), управление которым осуществляется через пользовательский интерфейс — консоль ЕЦУ.

ЕЦУ Dallas Lock 8.0 позволяет осуществлять централизованное управление такими модулями клиентов, как СЗИ Dallas Lock 8.0 редакций «К» и «С» (включая модули МЭ и СОВ), СЗИ НСД Dallas Lock Linux, СЗИ ВИ Dallas Lock редакции «Стандартная» и «Расширенная», СДЗ Dallas Lock и WAF Dallas Lock.

При работе с модулями СЗИ ВИ Dallas Lock доступны следующие возможности:

- завершение работы и перезагрузка модуля;
- отображение информации о состоянии модуля;
- синхронизация политик/пользователей;
- управление пользователями и группами пользователей на модуле;
- управление политиками безопасности;
- настройка неактивного режима работы модуля;
- управление заданиями:
  - проверка обновлений;
  - изменение параметров лицензии и технической поддержки;
  - сохранение конфигурации;
  - применение конфигурации;
  - получение отчета о конфигурации;
- сбор журналов модуля;
- отправка сигнализации об инцидентах безопасности.

Некоторые параметры безопасности могут быть настроены сразу для всего ДБ, некоторые — для отдельных клиентов.

ЕЦУ предназначен для использования на ТС, таких как: персональные компьютеры, портативные компьютеры (ноутбуки, планшеты), серверы и ТС с поддержкой виртуальных сред (по технологии VMware и пр.) и технологии Windows To Go[27], работающих на 64-битной архитектуре процессоров под управлением операционных систем семейства Windows и семейства GNU Linux. С подробным описанием ЕЦУ Dallas Lock можно ознакомиться в Инструкции по использованию ЕЦУ Dallas Lock RU.48957919.501410-01 И6 / RU.48957919.501410-02 И6.

10.1 Ввод СЗИ ВИ в ДБ ЕЦУ

Ввести модуль СЗИ ВИ Dallas Lock в Домен безопасности можно через Консоль Центра управления СЗИ ВИ Dallas Lock.

Внимание! При вводе модуля СЗИ ВИ Dallas Lock в ДБ должен быть соблюден ряд условий:

1. в ЛВС должен быть работающий сервер ЕЦУ;
2. между модулем и сервером ЕЦУ должен быть свободный обмен пакетами по TCP/IP порту 17900.

Внимание! После ввода модуля СЗИ ВИ Dallas Lock под управление ЕЦУ значения параметров безопасности подлежат синхронизации со значениями политик ЕЦУ для базовой группы «Нераспределенные объекты».

Для ввода модуля в ДБ через Консоль Центра управления СЗИ ВИ Dallas Lock необходимо:

1. убедиться, что сервер ЕЦУ доступен по сети;
2. запустить консоль СЗИ ВИ, подключиться к Центру управления СЗИ ВИ;
3. выбрать в дополнительном меню пункт «Параметры ЕЦУ» (рис. 309);

[27] Поддержка технологии Windows To Go осуществляется только для Консоли ЕЦУ Dallas Lock.

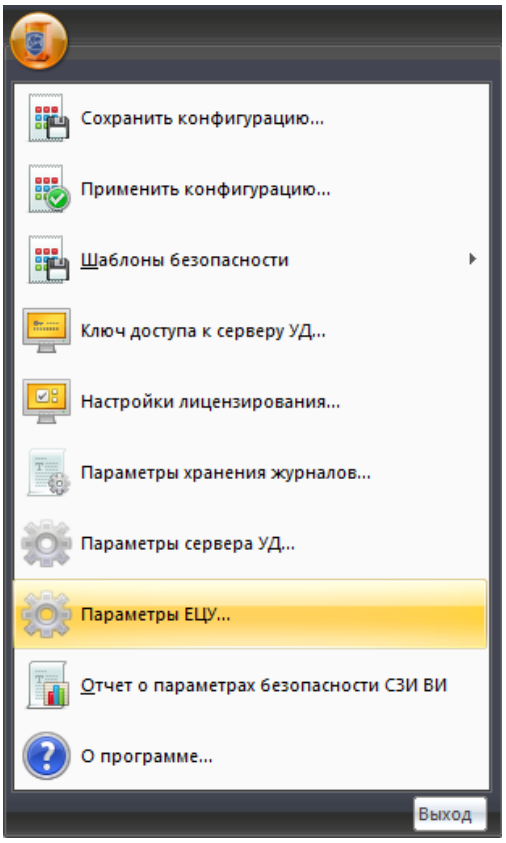


Рис. 309 – Ввод в ЕЦУ

4. в появившемся окне «Параметры ЕЦУ» поставить флаг в поле «под управлением ЕЦУ» и указать следующие данные (рис. 310):
   - DNS-имя или IP-адрес сервера ЕЦУ;
   - имя АРМ, в составе которого необходимо ввести модуль;
   - ключ доступа к ДБ ЕЦУ;

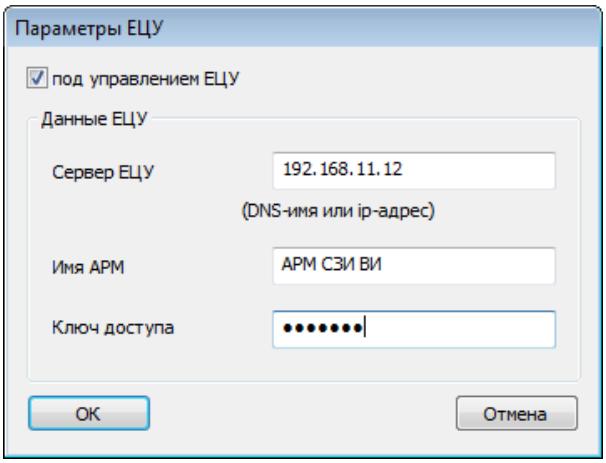


Рис. 310 – Окно «Ввод в ЕЦУ»

5. нажать кнопку «ОК», и будет инициировано создание АРМ и регистрация модуля в его составе (рис. 311).

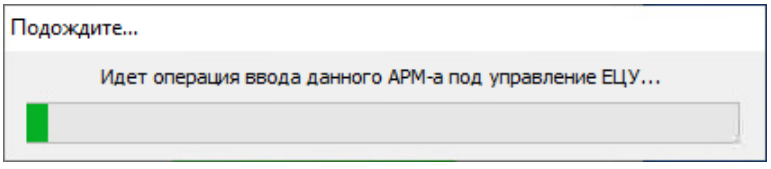


Рис. 311 – Операция ввода АРМ под управление ЕЦУ

Если процесс ввода модуля в ДБ прошел успешно, то через некоторое время появится соответствующее сообщение (рис. 312).

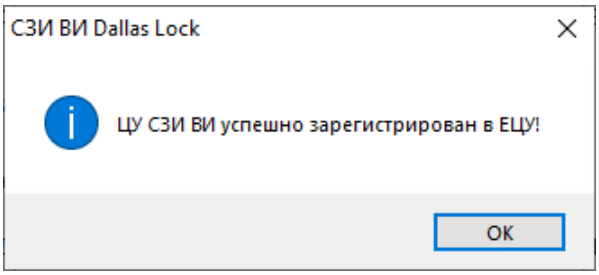


Рис. 312 – Модуль зарегистрирован в ЕЦУ

Примечание. Если во время процесса ввода модуля СЗИ ВИ Dallas Lock в ДБ возникает ошибка, содержащая текст «Ошибка регистрации в ЕЦУ! (Некорректные параметры вызова функции.)», то необходимо выполнить следующие действия:

- в настройках ЕЦУ (см. Инструкция по использованию ЕЦУ - «Общие параметры работы») в параметре «Способ подключения к серверу» установить значение «Оба способа» и выбрать приоритет подключения по IP-адресам;
- подождать 30 секунд для применения новых значений;
- повторить попытку ввода модуля СЗИ ВИ Dallas Lock в ДБ.

После при необходимости можно установить значение по умолчанию для параметра «Способ подключения к серверу» (оба способа с приоритетом подключения по полным доменным именам), на управление уже зарегистрированными в ДБ модулями СЗИ ВИ Dallas Lock это не повлияет.

10.2 Вывод СЗИ ВИ из ДБ ЕЦУ

Вывести модуль СЗИ ВИ Dallas Lock из Домена безопасности можно следующими способами:

- с помощью консоли ЕЦУ (см. Инструкция по использованию ЕЦУ – «Настройка модуля»);
- через Консоль Центра управления СЗИ ВИ Dallas Lock.

Для вывода модуля через Консоль Центра управления СЗИ ВИ Dallas Lock необходимо:

1. запустить консоль СЗИ ВИ, подключиться к Центру управления СЗИ ВИ;
2. выбрать в дополнительном меню пункт «Параметры ЕЦУ»;
3. в появившемся окне «Параметры ЕЦУ» убрать флаг в поле «под управлением ЕЦУ» и нажать кнопку «ОК».
4. в появившемся диалоговом окне нажать кнопку «Да», будет инициировано удаление АРМ из ДБ ЕЦУ (рис. 313);

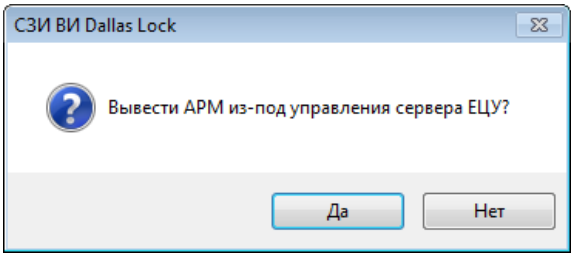


Рис. 313 – Вывод АРМ из-под управления сервера ЕЦУ

Если процесс вывода модуля из ДБ прошел успешно, то через некоторое время появится соответствующее сообщение (рис. 314).

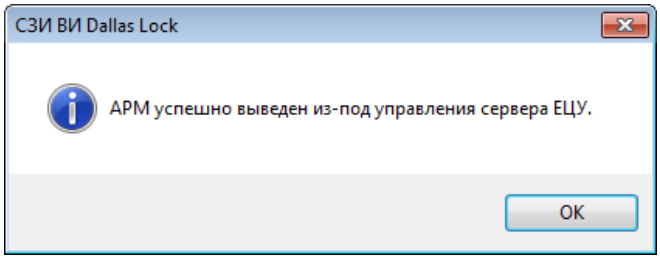


Рис. 314 – Модуль СЗИ ВИ выведен из ДБ ЕЦУ

В консоли ЕЦУ удаленный модуль переместится в базовую группу «Удаленные объекты» дерева ДБ.

11 ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ

11.1 Сохранение конфигурации ЦУ СЗИ ВИ

С помощью резервной копии файла конфигурации СЗИ ВИ позволяет быстро возобновить работу в случае сбоя или переустановки ЦУ СЗИ ВИ.

Внимание! Сохранение и применение файла конфигурации ЦУ СЗИ ВИ осуществляется только на соответствующем ЦУ СЗИ ВИ с соответствующей версией, на котором данная конфигурация была сформирована. Использовать данный механизм для обновления СЗИ ВИ на более старшую версию не рекомендуется. Подробнее про обновление см. п. 2.10 «Обновление системы защиты».

Для сохранения настроек ЦУ СЗИ ВИ необходимо открыть дополнительное меню Консоли и нажать кнопку «Сохранить конфигурацию» (рис. 315).

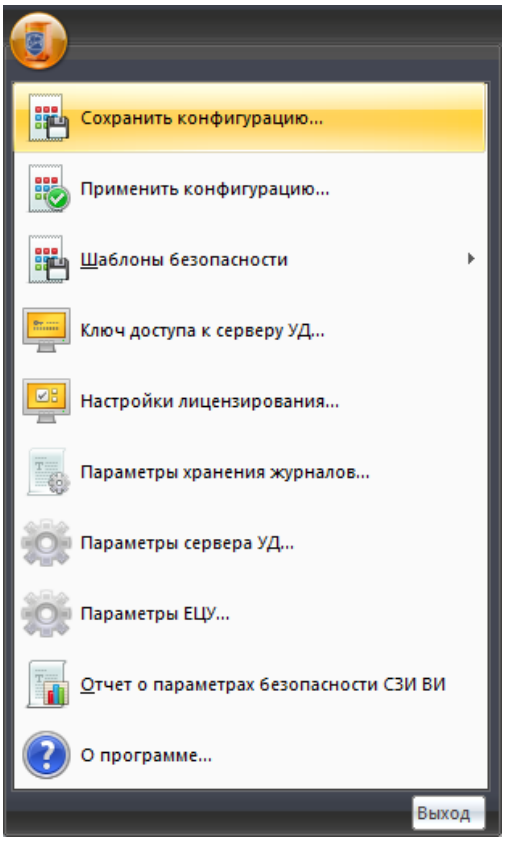


Рис. 315 – Меню Консоли

Появится окно, в котором необходимо выбрать расположение и имя файла, в котором будет сохранена конфигурация (по умолчанию – это системная папка «DLVI»). После нажатия кнопки «ОК» файл конфигурации ЦУ СЗИ ВИ будет сформирован и сохранен. Сохраненный файл конфигурации будет иметь расширение *.dlsc2.

Применяется данный файл конфигурации на уже установленный ЦУ СЗИ ВИ с помощью пункта «Применить конфигурацию» кнопки дополнительного меню Консоли.

11.2 Работа с логами

СЗИ ВИ позволяет получать расширенные логи в случае возникновения непредвиденных инцидентов для предоставления их технической поддержке.

Примечание. При предоставлении логов технической поддержке необходимо в сопроводительном письме предоставить подробное описание ситуации (окружение, время, порядок действий), при которой возникла та или иная нештатная ситуация (ошибка).

11.2.1 Включение логов виртуализации на ЦУ СЗИ ВИ и агентах Windows

(Hyper-V, vCenter for Windows)

Для сбора логов необходимо создать пустую папку «dlvilogs» по пути «C:\DLVI\Logs\». Таким образом логи будут находится по пути «C:\DLVI\Logs\dlvilogs\».

11.2.2 Включение логов НСД на ЦУ СЗИ ВИ и агентах Windows (Hyper-V, vCenter for Windows)

Для сбора логов необходимо создать пустую папку «1» по пути «C:\». Таким образом логи будут находится по пути «C:\1\».

11.2.3 Включение логов на агентах Linux (ESXi, vCSA, KVM/oVirt/zVirt/HOSTVM/РЕД Вирт)

Нужно создать файл /tmp/dlneedlog командой:

- "touch /tmp/dlneedlog".

Внимание! Файл пропадает после перезагрузки гипервизора/сервера виртуализации.

Далее необходимо выполнить рестарт агента DL:

- Для ESXi/vCSA - "/etc/init.d/confident-agentd restart";
- Для KVM/oVirt/zVirt/HOSTVM/РЕД Вирт - "systemctl restart confident-agentd".

Логи агента буду расположены по пути:

- Для ESXi - "/scratch/log/agentd.log";
- Для vCSA - "/etc/confident/agentd.log";
- Для KVM/oVirt/zVirt/HOSTVM/РЕД Вирт - "/etc/confident/agentd.log".

11.3 Настройки лицензирования

Сервер лицензий позволяет централизовать и упростить управление лицензиями на терминальные подключения и на клиентов в нескольких доменах безопасности (подробнее см. в документе «Инструкция по использованию сервера лицензий» ПФНА.501410.001 И4).

Для изменения параметров сервера лицензий для Сервера УД необходимо открыть дополнительное меню Консоли и нажать кнопку «Настройки лицензирования…» (рис. 318).

Появится окно «Настройки сервера лицензии для сервера УД». Для использования сервера лицензий, необходимо поставить флаг «Использовать сервер лицензий», заполнить параметры подключения к СЛ и ввести количество лицензий (рис. 316).

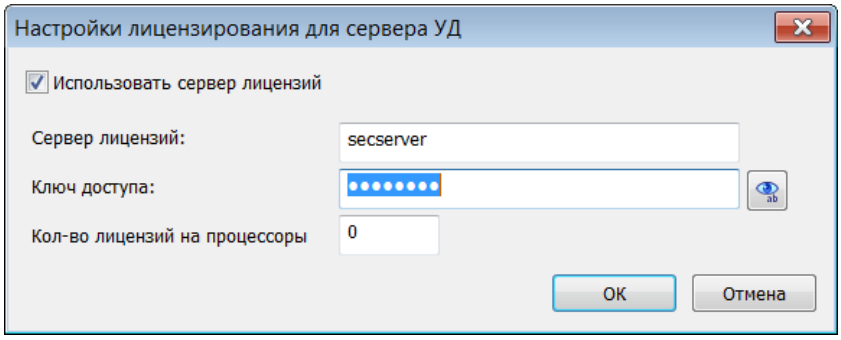


Рис. 316 – Настройка сервера лицензий для ЦУ СЗИ ВИ

Номера лицензий, коды технической поддержки, заведенные на клиентах, можно посмотреть на уровне Сервера УД, в категории «Состояние» → «Лицензии» (рис. 317).

Чтобы изменить параметры лицензии или внести код технической поддержки необходимо из списка выбрать клиента и в категории «Действия» нажать кнопку «Изменить параметры лицензии…». В появившемся окне ввести соответствующие данные и нажать кнопку «ОК».

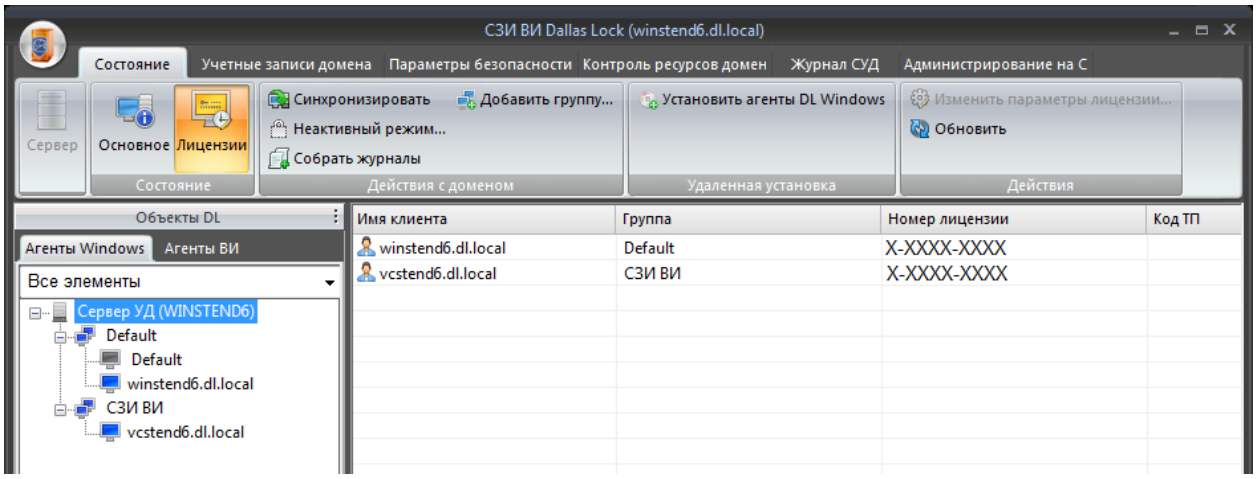


Рис. 317 – Просмотр лицензий

11.4 Шаблоны безопасности

В СЗИ ВИ Dallas Lock реализована возможность применения шаблонов безопасности, содержащих в себе конкретные настройки для СЗИ ВИ под требования нормативных документов. После установки выставлены настройки по умолчанию. Для применения шаблона безопасности в дополнительном меню Консоли необходимо навести курсор на пункт «Шаблоны безопасности» и в раскрывшемся меню правой кнопкой мыши выбрать пункт «Применить шаблон безопасности» (рис. 318).

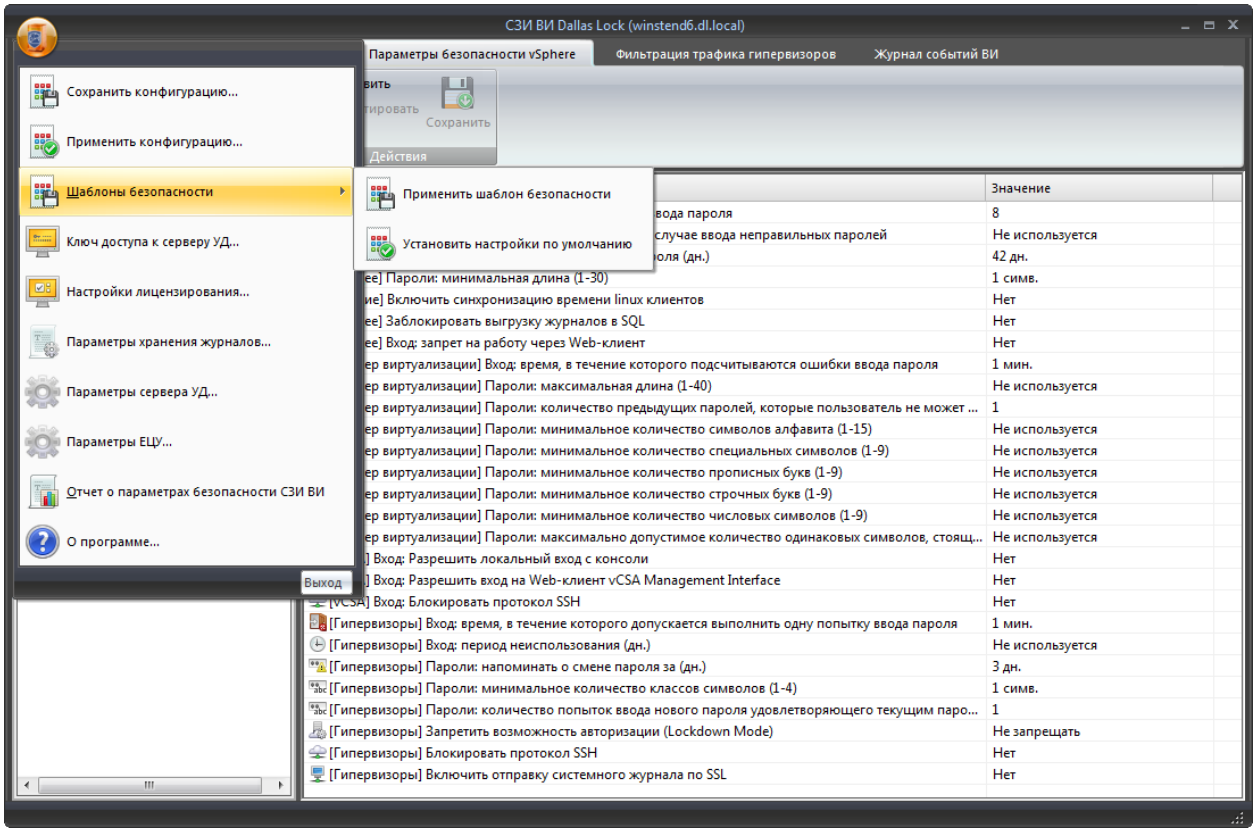


Рис. 318 – Шаблон безопасности

В появившемся окне установить флаг в поле с необходимым шаблоном безопасности, нажать кнопку «ОК» (рис. 319). При этом можно выбрать сразу несколько пунктов – шаблоны могут складываться, в таком случае при разных значениях одинаковых параметров, устанавливается самое ограничивающее значение.

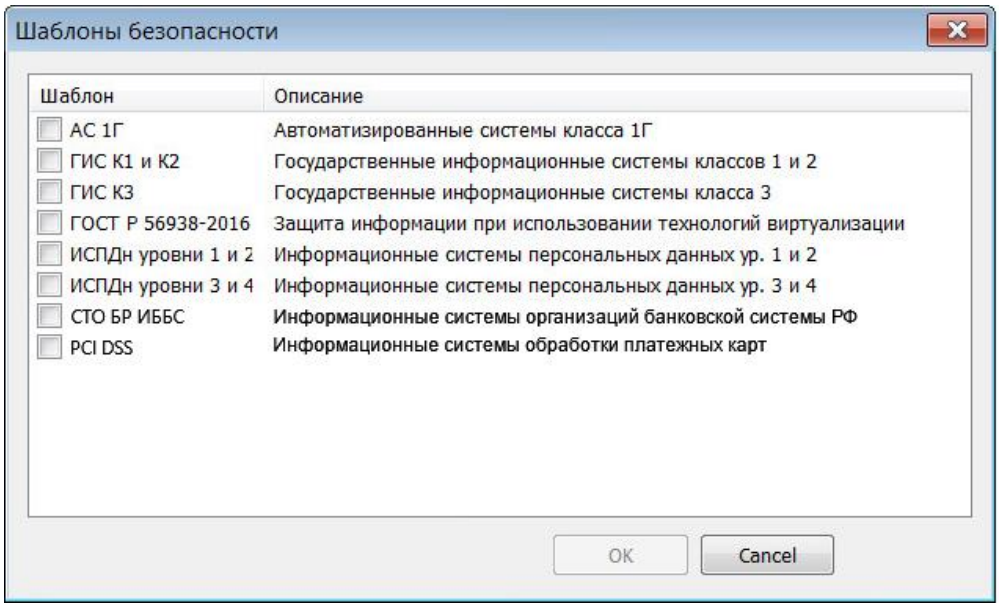


Рис. 319 – Выбор шаблона безопасности

Результатом произведенных действий будут настройки, выставленные в соответствии с требованиями выбранной политики безопасности. Перечень настроек приведен в приложении № 1.

11.5 Снапшоты

СЗИ ВИ Dallas Lock позволяет делать снимки состояния ВМ для платформ виртуализации vSphere и Hyper-V.

Внимание! СЗИ ВИ не контролирует количество снапшотов и занимаемый ими объем хранилищ, поэтому при создании автоматического сценария создания снапшотов, необходимо контролировать их количество и занимаемую ими память хранилища.

11.5.1 Ручное создание снапшота

Для создания снапшота необходимо:

1. Перейти на уровень СВ vSphere/Hyper-V или гипервизора ESXi и открыть категорию «Состояние» → «Управление снапшотами ВМ».
2. Выбрать из списка виртуальную машину.
3. Выбрать действие «Создать снапшот» (рис. 320).

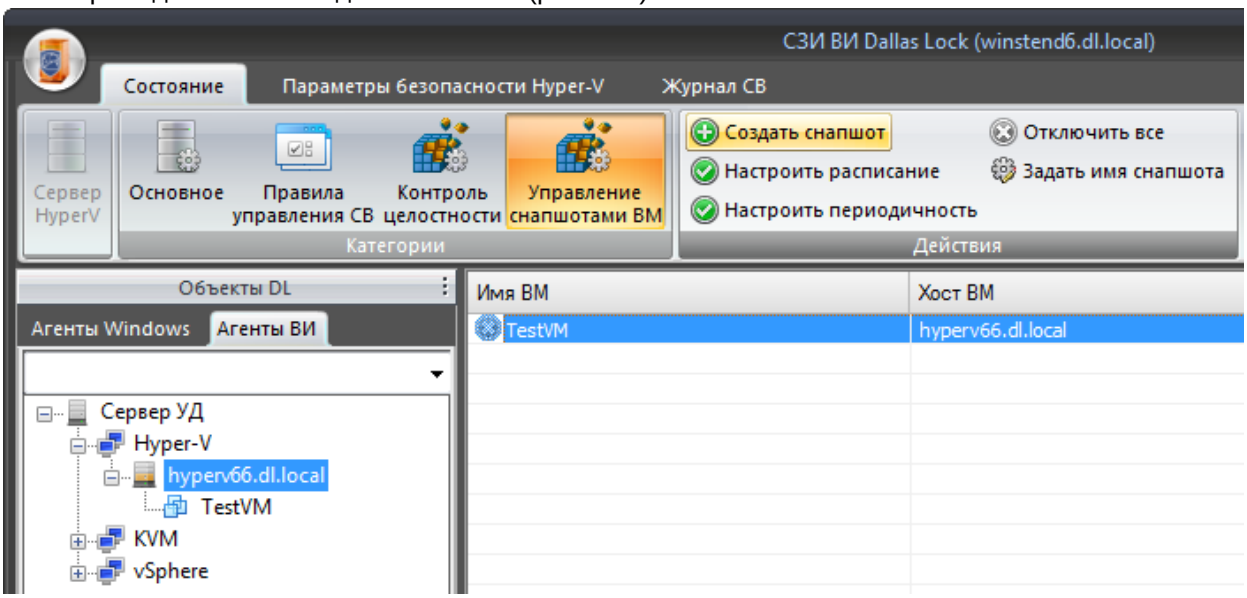


Рис. 320 – Создание снапшота

Или выбрать ВМ в дереве «Агенты ВИ» и выбрать соответствующий пункт в контекстном меню ВМ (рис. 321).

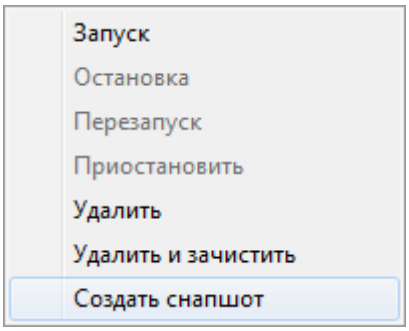


Рис. 321 – Контекстное меню ВМ

В случае успешного завершения отобразится сообщение «Снапшот создан».

11.5.2 Автоматическое снятие снапшотов

СЗИ ВИ Dallas Lock позволяет настроить автоматическое снятие снапшотов с заданной периодичностью и по расписанию.

Для настройки расписания снятия снапшотов необходимо:

1. Перейти на уровень СВ vSphere/Hyper-V или гипервизора ESXi и открыть категорию «Состояние» → «Управление снапшотами ВМ».
2. Выбрать из списка виртуальную машину.
3. Выбрать действие «Настроить расписание».
4. В появившемся окне задать необходимые параметры расписания снятия снапшотов (рис. 322).

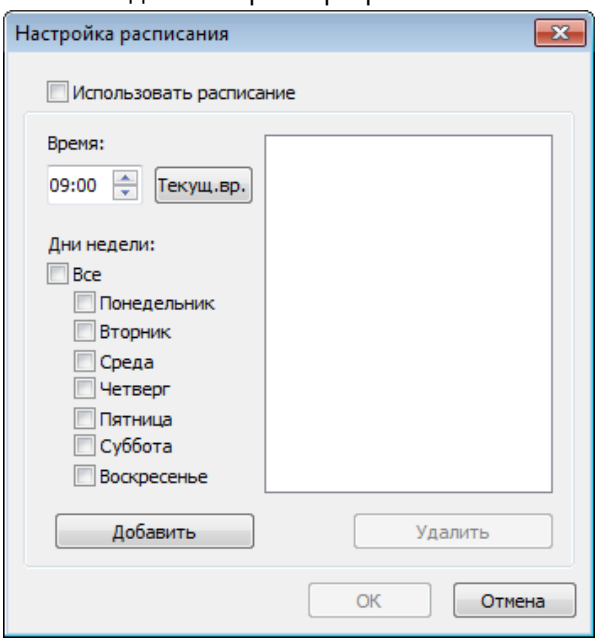


Рис. 322 – Настройка расписания

Для настройки периодичности снятия снапшотов необходимо:

1. Перейти на уровень СВ vSphere/Hyper-V или гипервизора ESXi и открыть категорию «Состояние» → «Управление снапшотами ВМ».
2. Выбрать из списка виртуальную машину.
3. Выбрать действие «Настроить периодичность».
4. В появившемся окне выбрать необходимый интервал снятия снапшотов (рис. 323).

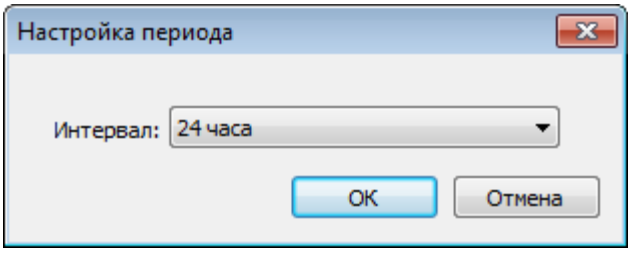


Рис. 323 – Контекстное меню ВМ

Для отключения всех настроенных параметров снятия снапшотов ВМ необходимо:

1. Перейти на уровень СВ vSphere/Hyper-V или гипервизора ESXi и открыть категорию «Состояние» → «Управление снапшотами ВМ».
2. Выбрать действие «Отключить все».

Для смены имени снапшотов по умолчанию необходимо:

1. Перейти на уровень СВ vSphere/Hyper-V или гипервизора ESXi и открыть категорию «Состояние» → «Управление снапшотами ВМ».
2. Выбрать действие «Задать имя снапшота» (рис. 324).
3. В появившемся окне указать имя, которое будет по умолчанию присваиваться создаваемым снапшотам.

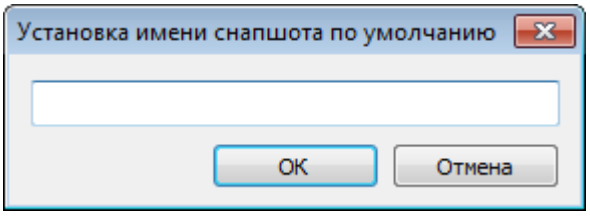


Рис. 324 – Установка имени снапшота по умолчанию

11.6 Создание отчета о параметрах безопасности и назначенных правах

СЗИ ВИ Dallas Lock позволяет сформировать отчет в формате RTF о параметрах безопасности, содержащий перечень защищаемых объектов, список пользователей/групп и их ролей, а также параметры политик безопасности.

Для создания отчета необходимо открыть дополнительное меню Консоли (рис. 318), выбрать пункт «Отчет о параметрах безопасности СЗИ ВИ», в появившемся окне задать путь к файлу и дождаться окончания процедуры экспорта. В случае успешного завершения отобразится сообщение «Отчет о параметрах безопасности СЗИ ВИ сформирован», сгенерированный файл станет доступен для просмотра.

Отчет начинается с перечня атрибутов:

- «Дата построения»;
- «Имя компьютера»;
- «Название подразделения»;
- «Наименование АС»;
- «Рабочее место»;
- «Операционная система»;
- «Версия Dallas Lock»;
- «Номер лицензии Dallas Lock»;
- «Максимальное кол-во терминальных сессий»;
- «Номер системного блока».

Далее следует информация о редакции СЗИ ВИ («Стандартная\Расширенная»), наличии подключения к ЕЦУ.

Последующие разделы содержат информацию о субъектах и объектах доступа домена безопасности, включая параметры безопасности хоста с установленным ЦУ СЗИ ВИ и параметры элементов домена: платформы виртуализации (Hyper-V, vSphere, KVM), установленные агенты, роли, политики безопасности.

11.7 Блокирование запуска ВМ

Агент DL ESXi блокирует включение ВМ с веб-интерфейса гипервизора. Поэтому, если сервер управления виртуализации (vCenter/vCSA) расположен непосредственно на защищенном гипервизоре как ВМ, и произошло аварийное отключение данной ВМ, то для обхода ограничения запуска непосредственно с веб-интерфейса гипервизора в командной строке необходимо выполнить команду "vim-cmd vmsvc/power.on <vmid>", где <vmid> это номер виртуальной машины сервера управления виртуализации (vCenter/vCSA), который можно найти с помощью команды "vim-cmd vmsvc/getallvms". При этом при включении ВМ будет зарегистрировано событие НСД.

Примечание. Для работы в командной строке гипервизора необходимо убедиться, что отключена политика «[Гипервизоры] Запретить возможность авторизации (Lockdown Mode)». Подробнее см. п. 5.3.1.1 «Параметры входа для vSphere».

12 АВАРИЙНОЕ ОТКЛЮЧЕНИЕ СЗИ ВИ В РУЧНОМ РЕЖИМЕ

В данном разделе описано осуществление аварийного удаления ядра системы защиты, агента DL Hyper-V, агента DL vCenter for Windows.

Для аварийного отключения СЗИ ВИ в ОС Windows 7/8/8.1/10/2008R2/2012/2012R2/2016/2019 необходимо получить доступ к файловой системе.

Для этого можно воспользоваться, в том числе, платформой восстановления Windows Recovery Environment (WinRE). WinRE может быть загружена с установочного диска операционной системы. Но можно воспользоваться встроенным инструментом восстановления, не требующим загрузки с CD. Для этого необходимо запустить меню дополнительных вариантов загрузки (перед началом загрузки ОС нажать F8 на клавиатуре) (рис. 325).

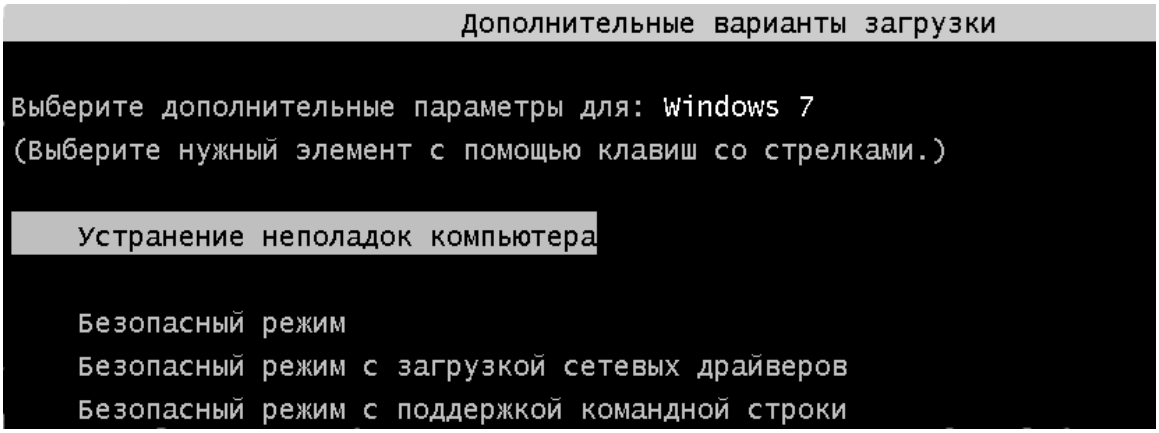


Рис. 325 - Меню дополнительных вариантов загрузки ОС Windows 7

Необходимо выбрать «Устранение неполадок компьютера» (Repair Your Computer). Windows загрузит необходимые файлы и запустит процесс восстановления. Система попросит выбрать язык и ввести авторизационные данные. Появится необходимое окно параметров восстановления системы. В нем следует выбрать открытие окна командной строки.

С помощью командной строки необходимо переключиться на диск (раздел жесткого диска), где установлена система защиты. Следует учесть, что буква того диска, который определен консолью восстановления как диск с установленной системой защиты, может не совпадать с буквой диска назначенного ОС, на который система защиты была установлена (диск C) (рис. 326).

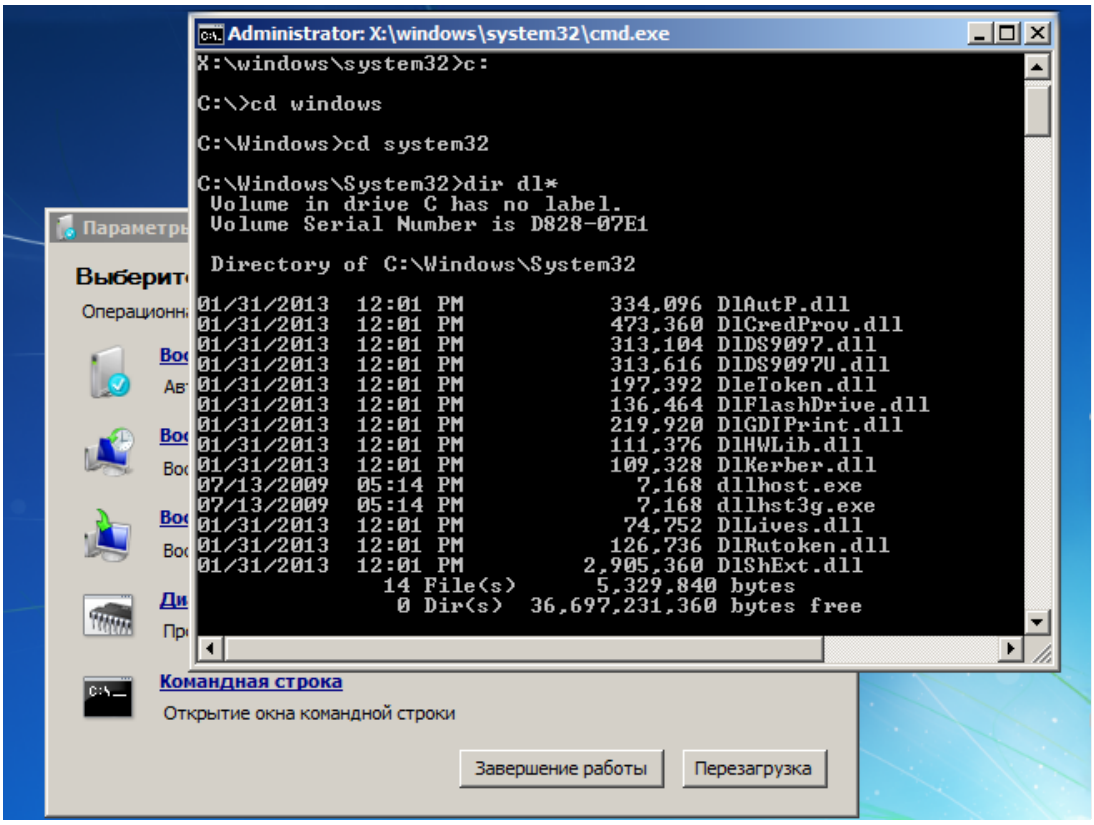


Рис. 326 - Консоль восстановления системы в Windows 7 и список системных файлов

Примечание. Следует учесть, что платформа восстановления WinRE имеется не на всех загрузочных дисках. Можно воспользоваться другими аварийно-восстановительными средствами получения прямого доступа к файловой системе в обход установленной ОС, например, Live CD Windows.

После получения доступа к файловой системе необходимо подменить системные файлы. После получения доступа к файловой системе необходимо зайти в папку System32 с помощью команды "cd %windir%\system32" и ввести следующие команды:

- "ren dlautp.dll dlautp_.dll";
- "copy msv1_0.dll dlautp.dll";
- "ren dlkerber.dll dlkerber_.dll";
- "copy kerberos.dll dlkerber.dll";
- "ren dllives.dll dllives_.dll";
- "copy livessp.dll dllives.dll"[28];
- "ren dlcloud.dll dlcloud_.dll" (только для Windows 10);
- "copy cloudAP.dll dlcloud.dll" (только для Windows 10).

Для отключения драйвера МЭ необходимо выполнить команду "cd %windir%\system32\drivers" и ввести следующие команды:

- "ren dlfirewall.sys dlfirewall.off".

После подмены системных файлов необходимо очистить реестр. После отключения модуля интерактивного входа для корректного отключения системы защиты необходимо внести изменения в реестр. Открыть редактор реестра можно с помощью командной строки командой "regedit" после ввода предыдущих команд. Можно открыть реестр из ОС, так как после подмены системных файлов компьютер должен успешно загрузиться (в поле ввода меню «Пуск» ввести команду "regedit"). В редакторе реестра следует проделать следующие операции»:

1. Изменить значение на «0» параметра «Disabled» по пути:
   - для Windows 7/2008R2
   «HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\{6f45dc1e-5384-457a-bc13-2cd81b0d28ed}»
   - для Windows 8/8.1/2012/2012R2/10/2016/2019

[28] Отсутствие файлов «dllives.dll» и «livessp.dll» не является критичным.

«HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\ {60b78e88-ead8-445c-9cfd-0b87f74ea6cd}».

2. Удалить ветку реестра «{9123E0C2-FF5E-4b38-BAB9-E2FA800D2548}» по пути «HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers».
3. Полностью удалить из реестра следующие разделы:
   - «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DlConv»;
   - «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DlDisk»;
   - «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DlFlt»;
   - «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DlHwCtrl»;
   - «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DlFireWall»;
   - «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DlLwf»;
   - «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DllPSService»;
   - «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_DLCONV»;
   - «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_DLFLTMGR»;
   - «HKEY_CLASSES_ROOT\DaLoDisk»;
   - «HKEY_CLASSES_ROOT\Dallas Lock coded data».

Для удаления разделов из ветки «Root» необходимо изменить права доступа для текущего пользователя (удобно сделать это не для каждого ключа, а для ветки «Root»).

4. Изменить значение ключа «UpperFilters» в ветке «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E967-E325-11CE-BFC1-08002BE10318}» вместо «DlDisk PartMgr» следует оставить «PartMgr».
5. Необходимо удалить значение «dlhwctrl» для ключей в ветке «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\...» в тех разделах, в которых он имеется. Для этого можно воспользоваться автопоиском по ветке реестра (функция «Найти…» в контекстном меню и кнопка F3 для перехода к следующей записи).
6. Необходимо удалить значение «DlDisk» для ключа UpperFilters в ветке «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class{4D36E965-E325-11CE-BFC1-08002BE10318}».
7. Необходимо удалить значение «DlDisk» для ключа UpperFilters в ветке «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class{4D36E980-E325-11CE-BFC1-08002BE10318}».
8. Необходимо изменить значение ключа UpperFilters в ветке «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class{4D36E96B-E325-11CE-BFC1-08002BE10318}» вместо «kbdclass DlFlt» следует оставить «kbdclass».
9. Необходимо переименовать файл Dlconv.sys, находящийся в папке по пути «C:\Windows\System32\drivers».

Примечание. При корректной загрузке ОС данные операции возможны и в режиме «Безопасный режим с поддержкой командной строки». В этом случае потребуется дополнительная авторизация в ОС Windows с правами администратора.

После выполнения вышеописанных операций необходимо перезагрузить компьютер. После перезагрузки система защиты будет отключена, теперь можно снова запустить ее установку, либо воспользоваться функцией «Восстановить» в окне установки и удаления программ.

Примечание. Для корректной установки СЗИ ВИ после ее аварийного отключения дополнительно необходимо удостовериться в отсутствии приложения «BlockIcon». Для этого нужно получить доступ в папку по пути «C:\Users\All users\Start Menu\Programs\Start Up» («C:\Documents and Settings\All users\Start Menu\Programs\Start Up» или «C:\Documents and Settings\All Users\Главное меню\Программы\Автозагрузка»). Сделать это можно, например, с помощью командной строки. В случае наличия «BlockIcon», его необходимо удалить.

13 Приложение № 1

Параметры, настраиваемые в политиках безопасности

1. Шаблон: По умолчанию

1.1. Windows

1.1.1. Вход

Параметр	Значение
Вход: запрет смены пользователя без перезагрузки	**Выкл.**
Вход: отображать имя последнего пользователя	**Да**
Вход: максимальное количество ошибок ввода пароля	**5**
Вход: время блокировки учетной записи в случае ввода неправильных паролей	**15 мин.**
Вход: отображать информацию о последнем успешном входе	**Нет**
Вход: разрешить использование смарт-карт	**Нет**
Вход: запретить использование парольного интерфейса входа	**Нет**
Вход: автоматический выбор аппаратного идентификатора при авторизации	**Нет**
Пароли: максимальный срок действия пароля	**42 дн.**
Пароли: минимальный срок действия пароля	**Не используется**
Пароли: напоминать о смене пароля за	**14 дн.**
Пароли: минимальная длина	**6 симв.**
Пароли: необходимо наличие цифр	**Нет**
Пароли: необходимо наличие спец. символов	**Нет**
Пароли: необходимо наличие строчных и прописных букв	**Нет**
Пароли: необходимо отсутствие цифры в первом и последнем символе	**Нет**
Пароли: необходимо изменение пароля не меньше, чем в	**Не используется**
Сеть: Ключ удаленного доступа	*****
Сеть: Время хранения сетевого кэша	**30 мин.**
Настройка считывателей аппаратных идентификаторов	**считыватели не настроены**
Блокировать компьютер при отключении аппаратного идентификатора	**Да**

1.1.2. Аудит

Параметр	Значение
Журнал входов в систему	**Вкл.**
Журнал ресурсов	**Вкл.**
Журнал управления политиками безопасности	**Вкл.**
Журнал управления учетными записями	**Вкл.**
Журнал запуска/завершения процессов	**Вкл.**
Журнал пакетов МЭ	**Выкл.**
Фиксировать в журнале входов неправильные пароли	**Нет**
Заносить в журнал исходящие попытки входа на удаленные компьютеры	**Нет**
Заносить в журнал события запуска и остановки ОС	**Да**
Заносить в журнал события запуска и остановки модулей администрирования DL	**Да**
Аудит устройств	**Выкл.**
Аудит событий зачистки	**Вкл.**
Аудит доступа: Заносить в журналы ошибки ОС	**Выкл.**
Аудит доступа/запуска: Вести аудит системных пользователей	**Выкл.**
Максимальное кол-во записей в журналах	**20000**

Периодическая архивация журналов	**Не используется**

1.1.3. Права пользователей

Параметр	Значение
Параметры безопасности: Управление	**Администраторы**
Учетные записи: Принудительная двухфакторная аутентификация	
Интерактивный вход: Разрешен	**Все**
Интерактивный вход: Запрещен	
Удаленный вход: Разрешен	**Все**
Удаленный вход: Запрещен	
Принудительное завершение работы по расписанию	
Деактивация системы защиты	

1.1.4. Очистка остаточной информации

Параметр	Значение
Очищать освобождаемое дисковое пространство	**Нет**
Очищать файл подкачки виртуальной памяти	**Нет**
Проверять очистку информации	**Нет**
Количество циклов затирания	**1**
Затирающая последовательность	**00 00 00 00**

1.1.5. Контроль целостности

1.1.5.1. Политики

Параметр	Значение
Проверять целостность ФС при загрузке ОС	**Вкл.**
Периодический контроль ФС	**Не используется**
Контроль ФС по расписанию	**Выкл.**
Проверять целостность прогр.апп. среды при загрузке ОС	**Вкл.**
Периодический контроль прогр.апп. среды	**Не используется**
Контроль прогр.апп. среды по расписанию	**Выкл.**
Проверять целостность реестра при загрузке ОС	**Вкл.**
Периодический контроль реестра	**Не используется**
Контроль реестра по расписанию	**Выкл.**
Изменение файлов с назначенным контролем целостности	**Разрешить**

1.1.5.2. Программно-аппаратная среда

Параметр	Значение
Контроль целостности прогр.апп. среды (Система)	**Выключено**
Контроль целостности прогр.апп. среды (Устройства ввода)	**Выключено**
Контроль целостности прогр.апп. среды (Принтеры)	**Выключено**
Контроль целостности прогр.апп. среды (Диски)	**Выключено**
Контроль целостности прогр.апп. среды (USB устройства)	**Выключено**
Контроль целостности прогр.апп. среды (Сеть)	**Выключено**
Контроль целостности прогр.апп. среды (Разделы диска)	**Выключено**
Контроль целостности прогр.апп. среды (BIOS)	**Выключено**
Контроль целостности прогр.апп. среды (Операционная система)	**Выключено**
Контроль целостности прогр.апп. среды (Драйверы)	**Выключено**
Контроль целостности прогр.апп. среды (Службы)	**Выключено**
Контроль целостности прогр.апп. среды (Программы)	**Выключено**
Контроль целостности прогр.апп. среды (Папки общего доступа)	**Выключено**

Контроль целостности прогр.апп. среды (Список пользователей)	**Выключено**

1.2. СЗИ ВИ (vSphere)

1.2.1. Вход

Параметр	Значение
[Общее] Вход: максимальное количество ошибок ввода пароля	**10**
[Общее] Вход: время блокировки учетной записи в случае ввода неправильных паролей	**Не используется**
[Общее] Пароли: максимальный срок действия пароля (дн.)	**180 дн.**
[Общее] Пароли: минимальная длина (1–30)	**6 симв.**
[Общие] Включить синхронизацию времени linux клиентов	**Да**
[Общие] Заблокировать выгрузку журналов в SQL	**Нет**
[Общее] Вход: запрет на работу через Web-клиент	**Нет**
[Сервер виртуализации] Вход: время, в течение которого подсчитываются ошибки ввода пароля	**1 мин.**
[Сервер виртуализации] Пароли: максимальная длина (1-40)	**20 симв.**
[Сервер виртуализации] Пароли: количество предыдущих паролей, которые пользователь не может использовать	**5**
[Сервер виртуализации] Пароли: минимальное количество символов алфавита (1–15)	**Не используется**
[Сервер виртуализации] Пароли: минимальное количество специальных символов (1–9)	**Не используется**
[Сервер виртуализации] Пароли: минимальное количество прописных букв (1–9)	**Не используется**
[Сервер виртуализации] Пароли: минимальное количество строчных букв (1–9)	**Не используется**
[Сервер виртуализации] Пароли: минимальное количество числовых символов (1–9)	**Не используется**
[Сервер виртуализации] Пароли: максимально допустимое количество одинаковых символов, стоящих рядом (1–5)	**3 симв.**
[Гипервизоры] Вход: время, в течение которого допускается выполнить одну попытку ввода пароля	**1 мин.**
[Гипервизоры] Вход: период неиспользования (дн.)	**1 дн.**
[Гипервизоры] Пароли: напоминать о смене пароля за (дн.)	**Не используется**
[Гипервизоры] Пароли: минимальное количество классов символов (1–4)	**Не используется**
[Гипервизоры] Вход: количество попыток ввода нового пароля, удовлетворяющего текущим парольным политикам	**3**
[Гипервизоры] Запретить возможность авторизации (Lockdown Mode)	**Не запрещать**
[Гипервизоры] Блокировать протокол SSH	**Нет**

1.2.2. Аудит

Параметр	Значение
[Общее] Агент сервера виртуализации vCenter	**Нет**
[Общее] ESXi Shell	**Нет**
[Общее] USB-устройства	**Нет**
[Общее] Аутентификация	**Нет**
[Общее] Системные события	**Нет**
[Общее] Виртуальные машины	**Нет**
[Общее] Зачистка ФС	**Нет**

1.2.3. Очистка остаточной информации

Параметр	Значение
[Гипервизоры] Количество циклов затирания	**1**

1.2.4. Настройка оповещения о событиях на клиентах (События НСД в дереве «Агенты Windows»)

Параметр	Значение
Нарушение контроля целостности	**Выкл.**
Попытка работы при нарушении целостности	**Выкл.**
Попытка нарушения целостности контролируемого объекта	**Выкл.**

1.2.5. Настройка оповещения событий на объектах ВМ (События НСД на вкладке СЗИ ВИ)

Параметр	Значение
Нарушение целостности системных файлов и аппаратной целостности ESXi/vCSA	**Выкл.**
Нарушение целостности файлов виртуальной машины	**Выкл.**
Попытка запуска виртуальной машины с нарушенной целостностью файлов	**Выкл.**
Попытка получения доступа при наличии ограничений сервера виртуализации	**Выкл.**

1.3. СЗИ ВИ (Hyper-V)

1.3.1. Аудит

Параметр	Значение
[Общее] Журнал гипервизора Hyper-V	**Нет**
[Уведомления] Журнал событий ВИ Hyper-V: управление ВМ	**Нет**
[Уведомления] Журнал событий ВИ Hyper-V: управление конфигурацией гипервизора	**Нет**
[Уведомления] Журнал событий ВИ Hyper-V: управление сетью	**Нет**
[Уведомления] Журнал событий ВИ Hyper-V: управление состоянием ВМ	**Нет**
[Уведомления] Журнал событий ВИ Hyper-V: управление конфигурацией ВМ	**Нет**
[Уведомления] Журнал событий ВИ Hyper-V: операции VMM	**Нет**

1.4. СЗИ ВИ (KVM)

1.4.1. Вход

Параметр	Значение
Вход: максимальное количество ошибок ввода пароля	**10**
Вход: время блокировки учетной записи в случае ввода неправильных паролей (сек.)	**Не используется**
Вход: блокировать протокол SSH	**Да**
Включить синхронизацию времени по NTP	**Да**
Заблокировать выгрузку журналов в SQL	**Нет**

2. Шаблон: АС 1Г

2.1. Windows

2.1.1. Вход

Параметр	Значение
Вход: запрет смены пользователя без перезагрузки	**Вкл.**
Вход: отображать имя последнего пользователя	**Да**
Вход: максимальное количество ошибок ввода пароля	**5**
Вход: время блокировки учетной записи в случае ввода неправильных паролей	**15 мин.**
Вход: отображать информацию о последнем успешном входе	**Нет**

Вход: разрешить использование смарт-карт	**Нет**
Вход: запретить использование парольного интерфейса входа	**Нет**
Вход: автоматический выбор аппаратного идентификатора при авторизации	**Нет**
Пароли: максимальный срок действия пароля	**42 дн.**
Пароли: минимальный срок действия пароля	**Не используется**
Пароли: напоминать о смене пароля за	**14 дн.**
Пароли: минимальная длина	**6 симв.**
Пароли: необходимо наличие цифр	**Да**
Пароли: необходимо наличие спец. символов	**Нет**
Пароли: необходимо наличие строчных и прописных букв	**Нет**
Пароли: необходимо отсутствие цифры в первом и последнем символе	**Нет**
Пароли: необходимо изменение пароля не меньше, чем в	**Не используется**
Сеть: Ключ удаленного доступа	*****
Сеть: Время хранения сетевого кэша	**30 мин.**
Настройка считывателей аппаратных идентификаторов	**считыватели не настроены**
Блокировать компьютер при отключении аппаратного идентификатора	**Да**

2.1.2. Аудит

Параметр	Значение
Журнал входов в систему	**Вкл.**
Журнал ресурсов	**Вкл.**
Журнал управления политиками безопасности	**Вкл.**
Журнал управления учетными записями	**Вкл.**
Журнал запуска/завершения процессов	**Вкл.**
Журнал пакетов МЭ	**Выкл.**
Фиксировать в журнале входов неправильные пароли	**Да**
Заносить в журнал исходящие попытки входа на удаленные компьютеры	**Нет**
Заносить в журнал события запуска и остановки ОС	**Да**
Заносить в журнал события запуска и остановки модулей администрирования DL	**Да**
Аудит устройств	**Вкл.**
Аудит событий зачистки	**Вкл.**
Аудит доступа: Заносить в журналы ошибки ОС	**Выкл.**
Аудит доступа/запуска: Вести аудит системных пользователей	**Выкл.**
Максимальное кол-во записей в журналах	**20000**
Периодическая архивация журналов	**Не используется**

2.1.3. Очистка остаточной информации

Параметр	Значение
Очищать освобождаемое дисковое пространство	**Да**
Очищать файл подкачки виртуальной памяти	**Да**
Количество циклов затирания	**1**

2.1.4. Контроль целостности

2.1.4.1. Политики

Параметр	Значение
Проверять целостность ФС при загрузке ОС	**Вкл.**
Проверять целостность прогр.апп. среды при загрузке ОС	**Вкл.**
Проверять целостность реестра при загрузке ОС	**Вкл.**
Изменение файлов с назначенным контролем целостности	**Разрешить**

2.2. СЗИ ВИ (vSphere)

2.2.1. Вход

Параметр	Значение
[Общее] Вход: максимальное количество ошибок ввода пароля	**5**
[Общее] Вход: время блокировки учетной записи в случае ввода неправильных паролей	**15 мин.**
[Общее] Пароли: максимальный срок действия пароля (дн.)	**42 дн.**
[Сервер виртуализации] Пароли: минимальное количество числовых символов (1–9)	**1 симв.**
[Общее] Пароли: минимальная длина (1–30)	**6 симв.**

2.2.2. Аудит

Параметр	Значение
[Общее] Агент сервера виртуализации vCenter	**Да**
[Общее] USB-устройства	**Да**
[Общее] Аутентификация	**Да**
[Общее] Системные события	**Да**
[Общее] Виртуальные машины	**Да**
[Общее] Зачистка ФС	**Да**

2.2.3. Очистка остаточной информации

Параметр	Значение
[Гипервизоры] Количество циклов затирания	**1**

2.3. СЗИ ВИ (Hyper-V)

2.3.1. Аудит

Параметр	Значение
[Общее] Журнал гипервизора Hyper-V	**Да**
[Уведомления] Журнал событий ВИ Hyper-V: управление ВМ	**Да**
[Уведомления] Журнал событий ВИ Hyper-V: управление состоянием ВМ	**Да**
[Уведомления] Журнал событий ВИ Hyper-V: управление конфигурацией ВМ	**Да**
[Уведомления] Журнал событий ВИ Hyper-V: управление сетью	**Да**
[Уведомления] Журнал событий ВИ Hyper-V: управление конфигурацией гипервизора	**Да**

2.4. СЗИ ВИ (KVM)

2.4.1. Вход

Параметр	Значение
Вход: максимальное количество ошибок ввода пароля	**10**

3. Шаблон: ГИС К1 и К2

3.1. Windows

3.1.1. Вход

Параметр	Значение
Вход: запрет смены пользователя без перезагрузки	**Вкл.**
Вход: максимальное количество ошибок ввода пароля	**5**
Вход: время блокировки учетной записи в случае ввода неправильных паролей	**15 мин.**
Пароли: максимальный срок действия пароля	**42 дн.**
Пароли: минимальная длина	**6 симв.**

3.1.2. Аудит

Параметр	Значение
Журнал входов в систему	**Вкл.**
Журнал ресурсов	**Вкл.**
Журнал управления политиками безопасности	**Вкл.**
Журнал управления учетными записями	**Вкл.**
Журнал запуска/завершения процессов	**Вкл.**
Журнал пакетов МЭ	**Выкл.**
Фиксировать в журнале входов неправильные пароли	**Да**
Заносить в журнал события запуска и остановки ОС	**Да**
Заносить в журнал события запуска и остановки модулей администрирования DL	**Да**
Аудит устройств	**Вкл.**
Аудит событий зачистки	**Вкл.**

3.1.3. Очистка остаточной информации

Параметр	Значение
Очищать освобождаемое дисковое пространство	**Да**
Очищать файл подкачки виртуальной памяти	**Да**
Количество циклов затирания	**1**

3.1.4. Контроль целостности

3.1.4.1. Политики

Параметр	Значение
Проверять целостность ФС при загрузке ОС	**Вкл.**
Проверять целостность прогр.апп. среды при загрузке ОС	**Вкл.**
Проверять целостность реестра при загрузке ОС	**Вкл.**
Изменение файлов с назначенным контролем целостности	**Разрешить**

3.2. СЗИ ВИ (vSphere)

3.2.1. Вход

Параметр	Значение
[Общее] Вход: максимальное количество ошибок ввода пароля;	**5**
[Общее] Вход: время блокировки учетной записи в случае ввода неправильных паролей	**15 мин.**
[Общее] Пароли: максимальный срок действия пароля (дн.)	**42 дн.**
[Общее] Пароли: минимальная длина (1–30)	**6 симв.**
[Гипервизоры] Запретить возможность авторизации (Lockdown Mode)	**При удаленном подключении**
[Гипервизоры] Блокировать протокол SSH	**Да**

3.2.2. Аудит

Параметр	Значение
[Общее] Агент сервера виртуализации vCenter	**Да**
[Общее] USB-устройства	**Да**
[Общее] Аутентификация	**Да**
[Общее] Системные события	**Да**
[Общее] Виртуальные машины	**Да**
[Общее] Зачистка ФС	**Да**

3.2.3. Очистка остаточной информации

Параметр	Значение

[Гипервизоры] Количество циклов затирания	**1**

3.2.4. Настройка оповещения о событиях на клиентах (События НСД в дереве «Агенты Windows»)

Параметр	Значение
Нарушение контроля целостности	**Вкл.**
Попытка работы при нарушении целостности	**Вкл.**
Попытка нарушения целостности контролируемого объекта	**Вкл.**

3.2.5. Настройка оповещения событий на объектах ВМ (События НСД на вкладке СЗИ ВИ)

Параметр	Значение
Нарушение целостности системных файлов и аппаратной целостности ESXi/vCSA	**Вкл.**
Нарушение целостности файлов виртуальной машины	**Вкл.**
Попытка запуска виртуальной машины с нарушенной целостностью файлов	**Вкл.**
Попытка получения доступа при наличии ограничений сервера виртуализации	**Вкл.**

3.3. СЗИ ВИ (Hyper-V)

3.3.1. Аудит

Параметр	Значение
[Уведомления] Журнал событий ВИ Hyper-V: управление ВМ	**Да**
[Уведомления] Журнал событий ВИ Hyper-V: управление конфигурацией гипервизора	**Да**
[Уведомления] Журнал событий ВИ Hyper-V: управление сетью	**Да**
[Уведомления] Журнал событий ВИ Hyper-V: управление состоянием ВМ	**Да**
[Уведомления] Журнал событий ВИ Hyper-V: управление конфигурацией ВМ	**Да**
[Общее] Журнал гипервизора Hyper-V	**Да**

3.4. СЗИ ВИ (KVM)

3.4.1. Вход

Параметр	Значение
Вход: максимальное количество ошибок ввода пароля	**10**

4. Шаблон: ГИС К3

4.1. Windows

4.1.1. Вход

Параметр	Значение
Вход: максимальное количество ошибок ввода пароля	**5**
Вход: время блокировки учетной записи в случае ввода неправильных паролей	**15 мин.**
Пароли: максимальный срок действия пароля	**42 дн.**
Пароли: минимальная длина	**6 симв.**

4.1.2. Аудит

Параметр	Значение
Журнал входов в систему	**Вкл.**
Журнал ресурсов	**Вкл.**
Журнал управления политиками безопасности	**Вкл.**
Журнал управления учетными записями	**Вкл.**
Журнал запуска/завершения процессов	**Вкл.**
Журнал пакетов МЭ	**Выкл.**

Фиксировать в журнале входов неправильные пароли	**Да**
Заносить в журнал события запуска и остановки ОС	**Да**
Заносить в журнал события запуска и остановки модулей администрирования DL	**Да**
Аудит устройств	**Вкл.**
Аудит событий зачистки	**Вкл.**

4.1.3. Очистка остаточной информации

Параметр	Значение
Очищать освобождаемое дисковое пространство	**Да**
Очищать файл подкачки виртуальной памяти	**Да**
Количество циклов затирания	**1**

4.1.4. Контроль целостности

4.1.4.1. Политики

Параметр	Значение
Проверять целостность ФС при загрузке ОС	**Вкл.**
Проверять целостность прогр.апп. среды при загрузке ОС	**Вкл.**
Проверять целостность реестра при загрузке ОС	**Вкл.**
Изменение файлов с назначенным контролем целостности	**Разрешить**

4.2. СЗИ ВИ (vSphere)

4.2.1. Вход

Параметр	Значение
[Общее] Вход: максимальное количество ошибок ввода пароля;	**5**
[Общее] Вход: время блокировки учетной записи в случае ввода неправильных паролей	**15 мин.**
[Общее] Пароли: максимальный срок действия пароля (дн.)	**42 дн.**
[Общее] Пароли: минимальная длина (1–30)	**6 симв.**

4.2.2. Аудит

Параметр	Значение
[Общее] Агент сервера виртуализации vCenter	**Да**
[Общее] USB-устройства	**Да**
[Общее] Аутентификация	**Да**
[Общее] Системные события	**Да**
[Общее] Виртуальные машины	**Да**
[Общее] Зачистка ФС	**Да**

4.2.3. Очистка остаточной информации

Параметр	Значение
[Гипервизоры] Количество циклов затирания	**1**

4.2.4. Настройка оповещения о событиях на клиентах (События НСД в дереве «Агенты Windows»)

Параметр	Значение
Нарушение контроля целостности	**Вкл.**
Попытка работы при нарушении целостности	**Вкл.**
Попытка нарушения целостности контролируемого объекта	**Вкл.**

4.2.5. Настройка оповещения событий на объектах ВМ (События НСД в дереве «Агенты ВИ»)

Параметр	Значение
Нарушение целостности системных файлов и аппаратной целостности	**Вкл.**

ESXi/vCSA	
Нарушение целостности файлов виртуальной машины	**Вкл.**
Попытка запуска виртуальной машины с нарушенной целостностью файлов	**Вкл.**
Попытка получения доступа при наличии ограничений сервера виртуализации	**Вкл.**

4.3. СЗИ ВИ (Hyper-V)

4.3.1. Аудит

Параметр	Значение
[Уведомления] Журнал событий ВИ Hyper-V: управление ВМ	**Да**
[Уведомления] Журнал событий ВИ Hyper-V: управление конфигурацией гипервизора	**Да**
[Уведомления] Журнал событий ВИ Hyper-V: управление сетью	**Да**
[Уведомления] Журнал событий ВИ Hyper-V: управление состоянием ВМ	**Да**
[Уведомления] Журнал событий ВИ Hyper-V: управление конфигурацией ВМ	**Да**
[Общее] Журнал гипервизора Hyper-V	**Да**

4.4. СЗИ ВИ (KVM)

4.4.1. Вход

Параметр	Значение
Вход: максимальное количество ошибок ввода пароля	**10**

5. Шаблон: ГОСТ Р 56938-2016

5.1. Windows

5.1.1. Аудит

Параметр	Значение
Журнал входов в систему	**Вкл.**
Журнал ресурсов	**Вкл.**
Журнал управления политиками безопасности	**Вкл.**
Журнал управления учетными записями	**Вкл.**
Журнал запуска/завершения процессов	**Вкл.**
Журнал пакетов МЭ	**Выкл.**
Фиксировать в журнале входов неправильные пароли	**Да**
Заносить в журнал события запуска и остановки ОС	**Да**
Заносить в журнал события запуска и остановки модулей администрирования DL	**Да**
Аудит устройств	**Вкл.**
Аудит событий зачистки	**Вкл.**

5.1.2. Очистка остаточной информации

Параметр	Значение
Очищать освобождаемое дисковое пространство	**Да**
Очищать файл подкачки виртуальной памяти	**Да**
Количество циклов затирания	**1**
Затирающая последовательность	**00 00 00 00**

5.1.3. Контроль целостности

5.1.3.1. Политики

Параметр	Значение
Проверять целостность ФС при загрузке ОС	**Вкл.**
Проверять целостность прогр.апп. среды при загрузке ОС	**Вкл.**
Проверять целостность реестра при загрузке ОС	**Вкл.**

Изменение файлов с назначенным контролем целостности	**Разрешить**

5.2. СЗИ ВИ (vSphere)

5.2.1. Вход

Параметр	Значение
[Гипервизоры] Запретить возможность авторизации (Lockdown Mode)	**При удаленном подключении**
[Гипервизоры] Блокировать протокол SSH	**Да**

5.2.2. Аудит

Параметр	Значение
[Общее] Агент сервера виртуализации vCenter	**Да**
[Общее] USB-устройства	**Да**
[Общее] Аутентификация	**Да**
[Общее] Системные события	**Да**
[Общее] Виртуальные машины	**Да**
[Общее] Зачистка ФС	**Да**

5.2.3. Очистка остаточной информации

Параметр	Значение
[Гипервизоры] Количество циклов затирания	**1**

5.2.4. Настройка оповещения о событиях на клиентах (События НСД в дереве «Агенты Windows»)

Параметр	Значение
Нарушение контроля целостности	**Вкл.**
Попытка работы при нарушении целостности	**Вкл.**
Попытка нарушения целостности контролируемого объекта	**Вкл.**

5.2.5. Настройка оповещения событий на объектах ВМ (События НСД в дереве «Агенты ВИ»)

Параметр	Значение
Нарушение целостности системных файлов и аппаратной целостности ESXi/vCSA	**Вкл.**
Нарушение целостности файлов виртуальной машины	**Вкл.**
Попытка запуска виртуальной машины с нарушенной целостностью файлов	**Вкл.**
Попытка получения доступа при наличии ограничений сервера виртуализации	**Вкл.**

5.3. СЗИ ВИ (Hyper-V)

5.3.1. Аудит

Параметр	Значение
[Уведомления] Журнал событий ВИ Hyper-V: управление ВМ	**Да**
[Уведомления] Журнал событий ВИ Hyper-V: управление конфигурацией гипервизора	**Да**
[Уведомления] Журнал событий ВИ Hyper-V: управление сетью	**Да**
[Уведомления] Журнал событий ВИ Hyper-V: управление состоянием ВМ	**Да**
[Уведомления] Журнал событий ВИ Hyper-V: управление конфигурацией ВМ	**Да**
[Общее] Журнал гипервизора Hyper-V	**Да**

5.4. СЗИ ВИ (KVM)

5.4.1. Вход

Параметр	Значение
Вход: максимальное количество ошибок ввода пароля	**10**

6. Шаблон: ИСПДн уровни 1 и 2

6.1. Windows

6.1.1. Аудит

Параметр	Значение
Журнал входов в систему	**Вкл.**
Журнал ресурсов	**Вкл.**
Журнал управления политиками безопасности	**Вкл.**
Журнал управления учетными записями	**Вкл.**
Журнал запуска/завершения процессов	**Вкл.**
Журнал пакетов МЭ	**Выкл.**
Фиксировать в журнале входов неправильные пароли	**Да**
Заносить в журнал события запуска и остановки ОС	**Да**
Заносить в журнал события запуска и остановки модулей администрирования DL	**Да**
Аудит устройств	**Вкл.**
Аудит событий зачистки	**Вкл.**

6.1.2. Контроль целостности

6.1.2.1. Политики

Параметр	Значение
Проверять целостность ФС при загрузке ОС	**Вкл.**
Проверять целостность прогр.апп. среды при загрузке ОС	**Вкл.**
Проверять целостность реестра при загрузке ОС	**Вкл.**
Изменение файлов с назначенным контролем целостности	**Разрешить**

6.2. СЗИ ВИ (vSphere)

6.2.1. Аудит

Параметр	Значение
[Общее] Агент сервера виртуализации vCenter	**Да**
[Общее] USB-устройства	**Да**
[Общее] Аутентификация	**Да**
[Общее] Системные события	**Да**
[Общее] Виртуальные машины	**Да**
[Общее] Зачистка ФС	**Да**

6.2.2. Настройка оповещения о событиях на клиентах (События НСД в дереве «Агенты Windows»)

Параметр	Значение
Нарушение контроля целостности	**Вкл.**
Попытка работы при нарушении целостности	**Вкл.**
Попытка нарушения целостности контролируемого объекта	**Вкл.**

6.2.3. Настройка оповещения событий на объектах ВМ (События НСД в дереве «Агенты ВИ»)

Параметр	Значение
Нарушение целостности системных файлов и аппаратной целостности ESXi/vCSA	**Вкл.**
Нарушение целостности файлов виртуальной машины	**Вкл.**
Попытка запуска виртуальной машины с нарушенной целостностью файлов	**Вкл.**
Попытка получения доступа при наличии ограничений сервера виртуализации	**Вкл.**

6.3. СЗИ ВИ (Hyper-V)

6.3.1. Аудит

Параметр	Значение
[Уведомления] Журнал событий ВИ Hyper-V: управление ВМ	**Да**
[Уведомления] Журнал событий ВИ Hyper-V: управление конфигурацией гипервизора	**Да**
[Уведомления] Журнал событий ВИ Hyper-V: управление сетью	**Да**
[Уведомления] Журнал событий ВИ Hyper-V: управление состоянием ВМ	**Да**
[Уведомления] Журнал событий ВИ Hyper-V: управление конфигурацией ВМ	**Да**
[Общее] Журнал гипервизора Hyper-V	**Да**

6.4. СЗИ ВИ (KVM)

6.4.1. Вход

Параметр	Значение
Вход: максимальное количество ошибок ввода пароля	**10**

7. Шаблон: ИСПДн уровни 3 и 4

7.1. Windows

7.1.1. Аудит

Параметр	Значение
Журнал входов в систему	**Вкл.**
Журнал ресурсов	**Вкл.**
Журнал управления политиками безопасности	**Вкл.**
Журнал управления учетными записями	**Вкл.**
Журнал запуска/завершения процессов	**Вкл.**
Журнал пакетов МЭ	**Выкл.**
Фиксировать в журнале входов неправильные пароли	**Да**
Заносить в журнал события запуска и остановки ОС	**Да**
Заносить в журнал события запуска и остановки модулей администрирования DL	**Да**
Аудит устройств	**Вкл.**
Аудит событий зачистки	**Вкл.**

7.1.2. Контроль целостности

7.1.2.1. Политики

Параметр	Значение
Проверять целостность ФС при загрузке ОС	**Вкл.**
Проверять целостность прогр.апп. среды при загрузке ОС	**Вкл.**
Проверять целостность реестра при загрузке ОС	**Вкл.**
Изменение файлов с назначенным контролем целостности	**Разрешить**

7.2. СЗИ ВИ (vSphere)

7.2.1. Аудит

Параметр	Значение
[Общее] Агент сервера виртуализации vCenter	**Да**
[Общее] USB-устройства	**Да**
[Общее] Аутентификация	**Да**
[Общее] Системные события	**Да**
[Общее] Виртуальные машины	**Да**
[Общее] Зачистка ФС	**Да**

7.2.2. Настройка оповещения о событиях на клиентах (События НСД в дереве «Агенты Windows»)

Параметр	Значение
Нарушение контроля целостности	**Вкл.**
Попытка работы при нарушении целостности	**Вкл.**
Попытка нарушения целостности контролируемого объекта	**Вкл.**

7.2.3. Настройка оповещения событий на объектах ВМ (События НСД в дереве «Агенты ВИ»)

Параметр	Значение
Нарушение целостности системных файлов и аппаратной целостности ESXi/vCSA	**Вкл.**
Нарушение целостности файлов виртуальной машины	**Вкл.**
Попытка запуска виртуальной машины с нарушенной целостностью файлов	**Вкл.**
Попытка получения доступа при наличии ограничений сервера виртуализации	**Вкл.**

7.3. СЗИ ВИ (Hyper-V)

7.3.1. Аудит

Параметр	Значение
[Уведомления] Журнал событий ВИ Hyper-V: управление ВМ	**Да**
[Уведомления] Журнал событий ВИ Hyper-V: управление конфигурацией гипервизора	**Да**
[Уведомления] Журнал событий ВИ Hyper-V: управление сетью	**Да**
[Уведомления] Журнал событий ВИ Hyper-V: управление состоянием ВМ	**Да**
[Уведомления] Журнал событий ВИ Hyper-V: управление конфигурацией ВМ	**Да**
[Общее] Журнал гипервизора Hyper-V	**Да**

7.4. СЗИ ВИ (KVM)

7.4.1. Вход

Параметр	Значение
Вход: максимальное количество ошибок ввода пароля	**10**

8. Шаблон: СТО БР ИББС

8.1. Windows

8.1.1. Вход

Параметр	Значение
Пароли: максимальный срок действия пароля	**30 дн.**
Пароли: необходимо наличие цифр	**Да**
Пароли: необходимо наличие строчных и прописных букв	**Да**
Вход: отображать информацию о последнем успешном входе	**Да**
Вход: время блокировки учетной записи в случае ввода неправильных паролей (мин.)	**30 мин.**

8.1.2. Аудит

Параметр	Значение
Фиксировать в журнале входов неправильные пароли	**Да**
Заносить в журнал исходящие попытки входа на удаленные компьютеры	**Да**
Аудит доступа/запуска: Вести аудит системных пользователей	**Вкл.**

8.1.3. Очистка остаточной информации

Параметр	Значение
Очищать освобождаемое дисковое пространство	**Да**
Очищать файл подкачки виртуальной памяти	**Да**

8.2. vSphere

8.2.1. Вход

Параметр	Значение
[Общее] Вход: максимальное количество ошибок ввода пароля	**5**
[Общее] Пароли: минимальная длина (1–30)	**7 симв.**
[Сервер виртуализации] Пароли: минимальное количество символов алфавита (0¬15)	**2**
[Сервер виртуализации] Пароли: минимальное количество прописных букв (1¬9)	**1**
[Сервер виртуализации] Пароли: минимальное количество строчных букв (1¬9)	**1**
[Сервер виртуализации] Пароли: минимальное количество числовых символов (1¬9)	**1**
[Гипервизоры] Пароли: напоминать о смене пароля за (дн.)	**5**
[Гипервизоры] Пароли: минимальное количество классов символов (1–4)	**3**

8.2.2. Аудит

Параметр	Значение
[Общее] Агент сервера виртуализации vCenter	**Да**
[Общее] ESXi Shell	**Да**
[Общее] Аутентификация	**Да**
[Общее] Системные события	**Да**
[Общее] Виртуальные машины	**Да**
[Общее] Зачистка ФС	**Да**
[Общее] Вход: время блокировки учетной записи в случае ввода неправильных паролей (мин.)	30 мин.

8.3. Настройка оповещения о событиях на клиентах (События НСД на вкладке «Агенты Windows»)

Параметр	Значение
Нарушение контроля целостности	**Вкл.**
Попытка работы при нарушении целостности	**Вкл.**
Попытка нарушения целостности контролируемого объекта	**Вкл.**

8.4. Настройка оповещения событий на объектах ВМ (События НСД на вкладке «Агенты ВИ»)

Параметр	Значение
Нарушение целостности системных файлов и аппаратной целостности ESXi/vCSA	**Вкл.**
Нарушение целостности файлов виртуальной машины	**Вкл**
Попытка запуска виртуальной машины с нарушенной целостностью файлов	**Вкл.**
Попытка получения доступа при наличии ограничений сервера виртуализации	**Вкл.**

8.1. vSphere

8.1.1. Настройка оповещения событий на объектах ВМ (События НСД на вкладке СЗИ ВИ)

Параметр	Значение
Нарушение целостности системных файлов и аппаратной целостности ESXi/vCSA	**Вкл.**
Нарушение целостности файлов виртуальной машины	**Вкл.**

8.1. Hyper-V

8.1.1. Аудит

Параметр	Значение
[Уведомления] Журнал событий ВИ Hyper-V: управление ВМ	**Да**

[Уведомления] Журнал событий ВИ Hyper-V: управление конфигурацией гипервизора	**Да**
[Уведомления] Журнал событий ВИ Hyper-V: управление сетью	**Да**
[Уведомления] Журнал событий ВИ Hyper-V: управление состоянием ВМ	**Да**
[Уведомления] Журнал событий ВИ Hyper-V: управление конфигурацией ВМ	**Да**
[Общее] Журнал гипервизора Hyper-V	**Да**

8.2. KVM

8.2.1. Вход

Параметр	Значение
Вход: максимальное количество ошибок ввода пароля	**5**

9. Шаблон: PCI DSS

9.1. Windows

9.1.1. Вход

Параметр	Значение
Пароли: максимальный срок действия пароля	**90 дн.**
Пароли: минимальная длина	**7 симв.**
Пароли: необходимо наличие цифр	**Да**
Пароли: необходимо наличие строчных и прописных букв	**Да**
Вход: время блокировки учетной записи в случае ввода неправильных паролей (мин.)	**30 мин.**

9.1.2. Аудит

Параметр	Значение
Журнал пакетов МЭ	**Вкл.**
Аудит устройств	**Вкл.**
Аудит событий зачистки	**Вкл.**

9.1.3. Очистка остаточной информации

Параметр	Значение
Очищать освобождаемое дисковое пространство	**Да**
Очищать файл подкачки виртуальной памяти	**Да**

9.2. vSphere

9.2.1. Вход

Параметр	Значение
[Общее] Пароли: максимальный срок действия пароля (дн.)	**90 дн.**
[Общее] Пароли: минимальная длина (1–30)	**7 симв.**
[Общее] Вход: время блокировки учетной записи в случае ввода неправильных паролей (мин.)	**30 мин.**
[Общее] Включить синхронизацию Linux клиентов	**Да**
[Сервер виртуализации] Пароли: минимальное количество символов алфавита (0¬15)	**2**
[Сервер виртуализации] Пароли: минимальное количество прописных букв (1¬9)	**1**
[Сервер виртуализации] Пароли: минимальное количество строчных букв (1¬9)	**1**
[Сервер виртуализации] Пароли: минимальное количество числовых символов (1¬9)	**1**
[Гипервизоры] Пароли: напоминать о смене пароля за (дн.)	**5**
[Гипервизоры] Пароли: минимальное количество классов символов (1–4)	**3**
[Гипервизоры] Запретить возможность авторизации (Lockdown Mode)	**при удаленном подключении**
[Гипервизоры] Блокировать протокол SSH	**Да**

9.2.2. Аудит

Параметр	Значение
[Общее] Агент сервера виртуализации vCenter	**Да**
[Общее] ESXi Shell	**Да**
[Общее] USB-устройства	**Да**
[Общее] Аутентификация	**Да**
[Общее] Системные события	**Да**
[Общее] Виртуальные машины	**Да**
[Общее] Зачистка ФС	**Да**

9.3. vSphere

9.3.1. Настройка оповещения о событиях на клиентах (События НСД в дереве «Агенты Windows»)

Параметр	Значение
Нарушение контроля целостности	**Вкл.**

9.3.2. Настройка оповещения событий на объектах ВМ (События НСД на вкладке СЗИ ВИ)

Параметр	Значение
Нарушение целостности системных файлов и аппаратной целостности ESXi/vCSA	**Вкл.**
Нарушение целостности файлов виртуальной машины	**Вкл.**

9.4. Hyper-V

9.4.1. Аудит

Параметр	Значение
[Уведомления] Журнал событий ВИ Hyper-V: управление ВМ	**Да**
[Уведомления] Журнал событий ВИ Hyper-V: управление конфигурацией гипервизора	**Да**
[Уведомления] Журнал событий ВИ Hyper-V: управление сетью	**Да**
[Уведомления] Журнал событий ВИ Hyper-V: управление состоянием ВМ	**Да**
[Уведомления] Журнал событий ВИ Hyper-V: управление конфигурацией ВМ	**Да**
[Общее] Журнал гипервизора Hyper-V	**Да**

9.5. Параметры сервера управления доступом:

Параметр	Значение
Синхронизация системного времени клиента	**Вкл.**

9.6. KVM

9.6.1. Вход

Параметр	Значение
[Общее] Вход: максимальное количество ошибок ввода пароля	**5**

14 Приложение № 2

14.1 Добавление корневого сертификата СЗИ ВИ в доверенные корневые сертификаты VMware PSC

Для обеспечения работоспособности политики [Гипервизоры] Включить отправку системного журнала по SSL этого необходимо:

1. В веб-браузере подключиться к PSC адресу https://psc_hostname_or_IP/psc. Во встроенном (embedded) PSC имя хоста или IP-адрес совпадает с именем хоста или IP-адресом сервера vCenter.
2. Ввести имя пользователя и пароль.
3. Выбрать пункт «Certificate Management».
4. Ввести IP-адрес или FQDN сервера, имя пользователя и пароль.
5. Во вкладе «Trust Root Certificates» нажать кнопку «Add certificate».
6. В появившемся окне указать путь к сертификату crt СЗИ ВИ. Сертификат crt находится на ТС с установленным ЦУ СЗИ ВИ в папке «C:\DLVI\VI\cert\<промежуточная папка>».

Далее необходимо выполнить операцию «Refresh CA Certificates» на хостах.

Для этого необходимо:

1. В веб-браузере подключиться к серверу vCenter
2. Ввести имя пользователя и пароль.
3. На уровне хоста перейти в категорию «Configure» → «System» → «Certificate».
4. Нажать кнопку «Renew» или «Refresh CA certificates».