



**ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО**  
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

**Программно-аппаратный комплекс «Сегмент-В.»**  
**(версия 1.3)**

# **Руководство администратора безопасности информации**

**11443195.4012.069 90**

Листов 30

**Москва**  
**2015**

## АННОТАЦИЯ

Настоящий документ является руководством администратора безопасности модуля разграничения доступа к vCenter и ESXi – программно-аппаратного комплекса (ПАК) «Сегмент-В.» v.1.3 (далее по тексту – «Сегмент-В.» или комплекс), предназначенного для защиты инфраструктуры виртуализации на основе VMware vSphere версий 5.1, 5.5, 6.0.

Документ предназначен для администратора безопасности информации – должностного лица, обладающего знаниями и полномочиями достаточными для того, чтобы контролировать безопасность инфраструктуры виртуализации VMware vSphere.

В документе приведены рекомендации по организации защиты инфраструктуры виртуализации с использованием средств комплекса «Сегмент-В.».

Перед началом эксплуатации ПАК «Сегмент-В.» рекомендуется внимательно ознакомиться с содержанием полного комплекта эксплуатационной документации, а также нормативными и методическими документами, регулирующими обеспечение информационной безопасности, включая политику безопасности информации предприятия или организации, эксплуатирующей комплекс.

Процесс установки и первичной настройки комплекса описан в «Руководстве по установке». «Руководство администратора» содержит описание дополнительных настроек, которые будут полезны в процессе дальнейшего администрирования комплекса.

Применение ПАК «Сегмент-В.» должно дополняться общими мерами предосторожности и физической безопасности.

## СОДЕРЖАНИЕ

<b>1. Общие сведения.....</b>	<b>5</b>
1.1. Назначение комплекса .....	5
1.2. Состав ПАК «Сегмент-В.».....	5
1.2.1. Аппаратные средства .....	6
1.2.2. Программные средства.....	6
1.3. Технические условия применения комплекса .....	7
<b>2. Установка и настройка компонентов комплекса .....</b>	<b>8</b>
<b>3. Администрирование аппаратной части ПАК «Сегмент-В.» .....</b>	<b>8</b>
<b>4. Администрирование СПО «Сегмент-В.» .....</b>	<b>8</b>
4.1. Общие сведения .....	8
4.2. Работа с утилитой управления комплексом «Segment-V.».....	9
4.2.1. Начало работы с утилитой.....	9
4.2.2. Работа с серверами.....	11
4.2.3. Работа с пользователями.....	12
4.2.4. Настройка меток безопасности .....	12
4.2.5. Назначение политик безопасности.....	12
4.2.6. Работа с группами .....	13
4.2.7. Работа с шаблонами.....	13
4.2.8. Работа с отчетами.....	13
4.3. Работа с сервисом регистрации событий .....	13
4.3.1. Общие сведения .....	13
4.3.2. Получение событий .....	14
4.3.3. Работа с фильтрами .....	17
4.3.4. Экспорт журнала .....	22
4.3.5. Просмотр статистики по полученным событиям.....	23
4.3.6. Настройки .....	24
4.4. Работа с утилитой «Installer-V.» .....	25
4.4.1. Добавление серверов в список защищаемых .....	25
4.4.2. Работа с утилитой в случае совместного использования «Сегмент-В.» и «Аккорд-В.» .....	26
4.4.3. Создание резервной копии и восстановление БД.....	27
<b>5. Работа на клиентских рабочих местах.....</b>	<b>29</b>
<b>6. Возможные затруднения в работе с ПАК «Сегмент-В.» и методы их устранения.....</b>	<b>29</b>
<b>7. Техническая поддержка и информация о комплексе .....</b>	<b>29</b>

## ПРИНЯТЫЕ ТЕРМИНЫ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

**Администратор БИ (или АБИ)** – администратор безопасности информации, привилегированный пользователь - должностное лицо, имеющее особый статус и абсолютные полномочия (супервизора). Администратор БИ организует установку комплекса в ПЭВМ, настройку защитных механизмов комплекса в соответствии с правами доступа пользователей, осуществляет контроль за правильным использованием ПЭВМ с установленным комплексом и периодическое тестирование средств защиты комплекса.

**Администратор ВИ (или АВИ)** – администратор виртуальной инфраструктуры, привилегированный пользователь - должностное лицо, отвечающее за настройку и обслуживание виртуальной инфраструктуры.

**АРМ** - автоматизированное рабочее место.

**Виртуальная машина (или VM)** – полностью изолированный программный контейнер, который работает с собственной операционной системой и приложениями подобно физическому компьютеру.

**Сервер виртуализации (или хост)** – объект виртуальной инфраструктуры, предоставляющий доступ к платформе виртуализации (гипервизору) посредством команд управления.

**Сервер управления виртуальной инфраструктурой (vCenter)** – сервер со специализированным программным обеспечением, отвечающий за распределение нагрузки в автоматическом режиме, перемещение виртуальных машин (миграцию) и настройку всех компонентов виртуализации посредством посылки команд управления остальным элементам виртуальной инфраструктуры.

**Сетевое устройство (сеть, группа портов)** – сеть, разделяемая между хостами и/или виртуальными машинами; может быть физической (подключена к физической сетевой карте) или логической (VLAN).

**Хранилище** – виртуальное представление физического хранилища, является местом хранения файлов виртуальных машин. Хранилище скрывает особенности своей физической реализации и предоставляет единую модель для хранения виртуальных машин.

**Пользователь** – субъект доступа к объектам (ресурсам) виртуальной инфраструктуры.

**Ошибки** – информация, выводимая на дисплей, указывающая на неправильность действий, сбои, аварии комплекса.

**Примечания** – замечания в описании некоторых команд, содержащие рекомендации администратору БИ по порядку использования этих команд. Пояснения выделены мелким шрифтом.

**Сообщения** - информация, выводимая на дисплей, которая сообщает о действиях, требуемых от пользователя, о состоянии программы и о корректно завершённых действиях.

## **1. Общие сведения**

### **1.1. Назначение комплекса**

Программно-аппаратный комплекс «Сегмент-В.» предназначен для защиты инфраструктур виртуализации, построенных на базе платформ виртуализации:

- VMware vSphere 5.1;
- VMware vSphere 5.5;
- VMware vSphere 6.0.

Комплекс представляет собой совокупность технических и программных средств, предназначенных для выполнения основных функций защиты от НСД на основе:

- идентификации и аутентификации субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации.
- управления доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре.
- регистрации событий безопасности в виртуальной инфраструктуре.
- управления перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных.
- разбиения виртуальной инфраструктуры на сегменты (сегментирования виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей.

### **1.2. Состав ПАК «Сегмент-В.»**

ПАК «Сегмент-В.» представляет собой комплекс программных и аппаратных средств, предназначенный для разграничения доступа пользователей к объектам инфраструктуры виртуализации VMware vSphere. При этом комплекс обеспечивает защиту от утечек информации, предоставляя возможность работы под одной учетной записью с различными сегментами виртуальной инфраструктуры (ВИ), запрещая их смешивание.

Основу комплекса составляет прокси-сервер, устанавливаемый в разрыв между vCenter сервером и рабочим местом администратора виртуальной инфраструктуры (АВИ).

Прокси-сервер представлен в следующих исполнениях:

- 1) аппаратное исполнение: физический сервер с предустановленным ПО;
- 2) программное исполнение: ISO-образ, предназначенный:
  - для установки в ВМ;
  - для установки на сторонний сервер организации-Заказчика.

**ВНИМАНИЕ!** В случае использования варианта исполнения, предназначенного для установки на сторонний сервер организации-Заказчика, следует учитывать, что аппаратная часть стороннего сервера должна быть совместима с базовой сборкой CentOS 6.5 и поддерживать работу с «Аккорд-АМДЗ».

«Сегмент-В.» не требует установки дополнительного ПО на АРМ администраторов виртуальной инфраструктуры и позволяет «бесшовно» интегрировать систему защиты в инфраструктуру виртуализации vSphere. При этом поддерживается режим Linked mode для vCenter, а также сохраняется возможность использования vCenter в качестве ВМ (в том числе VCSA – VMware vCenter Server Appliance).

ПАК «Сегмент-В.» состоит из аппаратных и программных средств.

### **1.2.1. Аппаратные средства**

Аппаратные средства ПАК «Сегмент-В.» включают в себя следующие компоненты:

- физический сервер Aquarius T40 S24 (опционально; возможны варианты использования собственных серверов);
- установленная в сервер (Aquarius T40 S24 или собственный сервер) плата «Аккорд-АМДЗ» семейства GX (подробнее см. документацию на «Аккорд-АМДЗ»);
- usb -> Ethernet адаптер – поставляется (опционально) в составе решения для использования функционала отказоустойчивости (High Availability).

### **1.2.2. Программные средства**

Программные средства ПАК «Сегмент-В.» включают в себя следующие компоненты:

#### **1) модули СПО «Сегмент-В.»:**

а) *ПО управления комплексом Segment-V. (exe)*, устанавливаемое на АРМ Администратора БИ (АРМ АБИ), предназначенное для настройки разграничения доступа к виртуальной инфраструктуре. Может устанавливаться отдельно или как расширение «СПО Аккорд-В.». Включает в себя следующие утилиты:.

- «Segment-V.» – утилита управления комплексом «Сегмент-В.»;
- «Installer-V.» – утилита настройки соединения с vCenter, а также точек сбора событий с прокси-серверов (в случае совместного использования с «Аккорд-В.» используется также для установки агентов «Аккорд-В.» на ESXi);
- «LogViewer-V.» – утилита просмотра зарегистрированных событий.

б) *сервис регистрации событий*, устанавливаемый на АРМ АБИ или в ОС отдельного сервера (рекомендуемый вариант), предназначенный для сбора событий инфраструктуры VMware vSphere, а также с агентов «Аккорд-В.» на ESXi (для установки сервиса регистрации событий в ОС предназначена вспомогательная утилита LogServiceInstaller);

**2) Segment-V. Module (iso)** – прокси-сервер – специально настроенный образ операционной системы, устанавливаемый на физический сервер или внутрь VM, предназначенный для перехвата команд управления vCenter/ESXi и организации разграничения доступа на основе заранее заданных правил Segment-V. Module включает в себя СПО «Аккорд-Х», применение которого на прокси-сервере обеспечивает выполнение процедур идентификации и аутентификации пользователей root и accord, а также выполнение динамического контроля целостности исполняемых файлов из состава ПАК «Сегмент-В.»..

*Примечание: В случае программного исполнения (VM), в силу невозможности использования контроллеров «Аккорд-АМДЗ», рекомендуется использовать ПАК «Аккорд-В.».*

### **1.3. Технические условия применения комплекса**

Для установки комплекса «Сегмент-В.» требуется следующий минимальный состав технических и программных средств:

- наличие инфраструктуры виртуализации, построенной на базе одной из поддерживаемых платформ виртуализации, список которых приведен в подразделе 1.1;
- реализация АРМ АБИ в виде физической машины под управлением ОС Windows, в которой установлены:
  - программная платформа Microsoft .NET Framework 3.5;
  - распространяемые пакеты (Redistributable Package) Microsoft Visual C++ 2008 (x86) и Microsoft Visual C++ 2010 (x86)<sup>1</sup>;
- наличие ресурсов на сервере для создания VM и установки в нее ОС прокси-сервера или наличие x86-64 совместимого сервера<sup>2</sup> с требованиями, аналогичными предъявляемым к VM.

Минимальные системные требования к VM:

- двухъядерный процессор, 2 Гб ОЗУ, 16 Гб свободного места на диске;
- две сетевых карты (E1000) – в случае использования одного прокси-сервера;
- три сетевых карты (E1000) – в случае использования механизмов резервирования;
- USB контроллер – для подключения устройства хранения с сертификатами;

Для корректной работы сервиса регистрации событий может потребоваться, чтобы АРМ, на котором он запущен, был включен в домен (если АРМ совпадает с vCenter, то возможно использование локальной учетной записи) (подробнее см. «Руководство по установке» (11443195.4012.069 98)).

---

<sup>1)</sup> Данные компоненты включены в комплект поставляемого ПО ПАК «Сегмент-В.»

<sup>2)</sup> В зависимости от варианта исполнения ПАК «Сегмент-В.», может входить в комплект поставки

Необходимо организовать схему подключения, при которой все запросы к vCenter и ESXi будут проходить через прокси-сервер (чтобы не существовало путей в обход модуля «Сегмент-В.»).

## 2. Установка и настройка компонентов комплекса

Установка и первичная настройка компонентов ПАК «Сегмент-В.» проводится в соответствии с положениями «Руководства по установке» (11443195.4012.069-98), входящего в состав комплекта поставки комплекса.

## 3. Администрирование аппаратной части ПАК «Сегмент-В.»

Процедуры администрирования аппаратной части («Аккорд-АМДЗ») описаны в соответствующих разделах документации, входящей в комплект поставки комплекса «Аккорд-АМДЗ»: см. «Руководство по установке» (11443195.4012-038 98), «Руководство администратора» (11443195.4012-038 90).

## 4. Администрирование СПО «Сегмент-В.»

### 4.1. Общие сведения

**ВНИМАНИЕ!** Информация, необходимая для установки и первоначальной настройки комплекса «Сегмент-В.», содержится в «Руководстве по установке». Настоящее руководство содержит описание дополнительных настроек ПО «Сегмент-В.», которые могут понадобиться в процессе дальнейшей эксплуатации.

Для администрирования СПО «Сегмент-В.» используются следующие компоненты управления:

- **«Installer-V.»** – утилита настройки соединения с vCenter, а также точек сбора событий с прокси-серверов (в случае совместного использования с «Аккорд-В.» используется также для установки агентов «Аккорд-В.» на ESXi);
- **«Segment-V.»** – утилита управления комплексом «Сегмент-В.»;
- **«LogViewer-V.»** – утилита просмотра зарегистрированных событий.



## 4.2. Работа с утилитой управления комплексом «Segment-V.»

### 4.2.1. Начало работы с утилитой

Для начала работы с утилитой управления комплексом следует на АРМ АБИ запустить с правами администратора утилиту «**Segment-V.**» и выполнить процедуру авторизации АБИ в системе (подробнее см. также подраздел «Настройка правил разграничения доступа» «Руководства по установке» (11443195.4012.069 98)). В появившемся окне уже будет заполнено поле «Сервер», содержащее IP-адрес vCenter, с которым будет происходить работа. Необходимо заполнить параметры учетной записи АБИ, и нажать кнопку <Вход>.

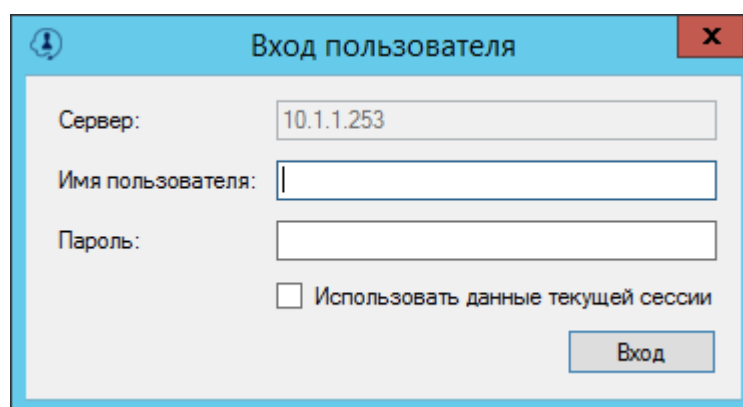


Рисунок 1 - Авторизация АБИ

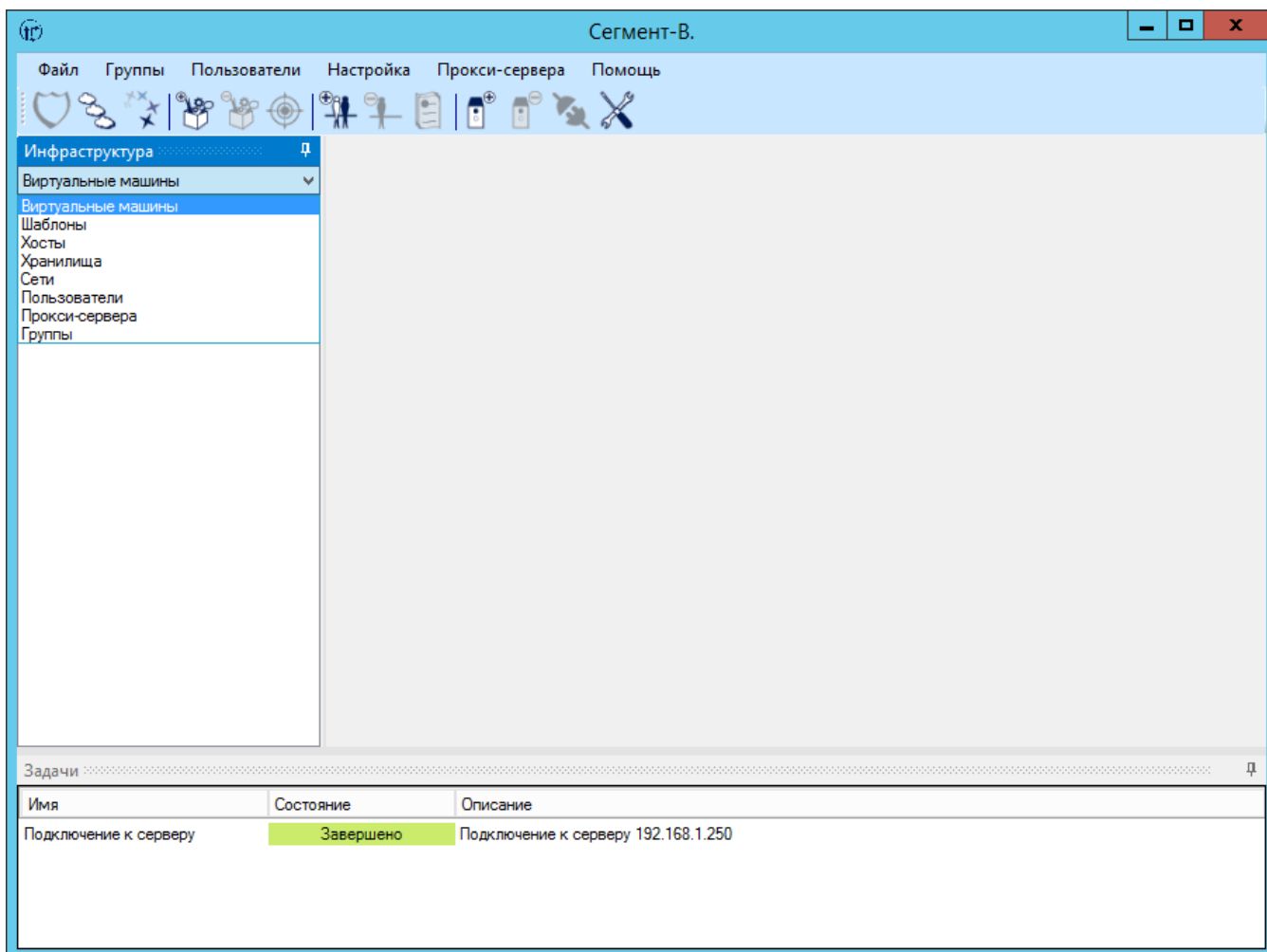
При запуске утилиты автоматически происходит подключение ко всем добавленным прокси-серверам.

После авторизации на экран выводится главное окно утилиты управления комплексом (рисунок 2), содержащее **на панели задач ряд кнопок**, подробные сведения о которых отражены в таблице 1.

Таблица 1 - Описание элементов панели задач главного окна утилиты «Segment-V.»

Название кнопки	Назначение	Примечание
<Назначить метки>	назначение меток безопасности пользователям и объектам виртуальной инфраструктуры	подробнее см. п. «Назначение политик безопасности» «Руководства по установке» (11443195.4012.069 98)
<Настроить уровни>	создание, изменение, удаление уровней доступа (иерархических меток безопасности)	подробнее см. п. «Настройка меток безопасности» «Руководства по установке» (11443195.4012.069 98)
<Настроить категории>	создание, изменение, удаление категорий доступа (неиерархических меток безопасности)	
<Добавить группу>	создание групп объектов для назначения им одинаковых меток	подробнее см. п. «Работа с группами» «Руководства по установке» (11443195.4012.069 98)
<Удалить группу>	удаление группы	
<Добавить в группу>	добавление объектов виртуальной инфраструктуры (ВМ, пользователи, сети, хосты, хранилища, шаблоны)	
<Добавить>	создание пользователя	подробнее см. п. «Добавление

Название кнопки	Назначение	Примечание
пользователя>		пользователей» «Руководства по установке» (11443195.4012.069 98)
<Удалить пользователя>	удаление пользователя	
<Операции>	настройка операций, разрешенных пользователю	подробнее см. п. «Назначение политик безопасности» «Руководства по установке» (11443195.4012.069 98)
<Добавить сервер>	создание прокси-сервера	подробнее см. п. «Настройка ПО управления» «Руководства по установке» (11443195.4012.069 98)
<Удалить сервер>	удаление прокси-сервера	
<Подключить>	подключение прокси-сервера	
<Настройка>	выбор режима работы прокси-серверов	подробнее см. п. «Назначение политик безопасности» «Руководства по установке» (11443195.4012.069 98)



**Рисунок 2 - Главное окно утилиты управления комплексом**

В разделе <Инфраструктура> отображаются все доступные для изменения и настройки элементы виртуальной системы. К ним относятся:

- виртуальные машины;
- шаблоны;

- хосты;
- хранилища;
- сети (группы портов и распределенные группы портов);
- пользователи;
- прокси-серверы (серверы безопасности);
- группы.

Для элементов инфраструктуры предусмотрены индикаторы состояний:

**1. Для виртуальных машин:**

- зеленый маркер – назначение меток разрешено, ВМ выключена;
- красный маркер – назначение меток ВМ разрешено, ВМ включена;
- желтый маркер – назначение меток ВМ разрешено, ВМ в состоянии «Suspend»;
- имя ВМ отмечено серым – ВМ удалена или конвертирована в шаблон;
- имя ВМ отмечено красным – недостаточно информации о ВМ (например, ВМ находится в одном из статусов orphaned, inaccessible, unknown, disconnected).

**2. Для шаблонов:**

- зеленый маркер – назначение меток разрешено;
- имя отмечено серым – шаблон удален или конвертирован в ВМ;

**3. Для хостов, хранилищ и сетей:**

- всегда зеленый маркер;
- имя отмечено серым – объект удален;
- имя отмечено красным – недостаточно информации об объекте (например, находится в одном из статусов orphaned, inaccessible, unknown, disconnected).

**4. Для пользователей:**

- всегда зеленый маркер.

**5. Для серверов безопасности (прокси-серверов):**

- зеленый маркер – соединение с сервером установлено;
- красный маркер – соединение с сервером не установлено.

В случае если ВМ, шаблон, хранилище, сеть или хост были удалены, они помечаются серым цветом как неактивные. При следующем включении ПО управления они уже не будут отображаться в списке.

**4.2.2. Работа с серверами**

Для настройки связи между прокси-серверами и ПО управления «Сегмент-В.» следует выполнить процедуру добавления и подключения прокси-серверов.

Подробное описание работы с прокси-серверами см. в п. «Настройка ПО управления» «Руководства по установке» (11443195.4012.069 98).

### 4.2.3. Работа с пользователями

**ВНИМАНИЕ!** ПО «Сегмент-В.» не создает своих пользователей в инфраструктуре VMware, а только разрешает/запрещает доступ пользователям, уже созданным в рамках VMware.

Добавить пользователя можно двумя способами:

- 1) добавить пользователя вручную;
- 2) загрузить пользователей из домена.

Подробное описание процедуры добавления пользователей см. в п. «Добавление пользователей» «Руководства по установке» (11443195.4012.069 98).

### 4.2.4. Настройка меток безопасности

«Сегмент-В.» позволяет создавать и работать с иерархическими (уровнями) и неиерархическими метками (категориями).

Разрешено создание 64 различных уровней иерархии (при создании иерархической метки задается его имя и уровень: от 1 до 64) и неограниченное количество категорий (для которых задается имя и цвет).

Подробное описание процедуры настройки меток безопасности см. п. «Настройка меток безопасности» «Руководства по установке» (11443195.4012.069 98).

### 4.2.5. Назначение политик безопасности

Работа через vClient подразумевает в качестве действий операции, которые могут затрагивать один или несколько объектов доступа. Объектами доступа в ПО «Сегмент-В.» являются хосты, ВМ, шаблоны, сети (группы портов, распределенные группы портов) и хранилища. Примерами операций могут служить: включение ВМ, миграция ВМ со сменой хоста и/или хранилища, переименование и так далее.

Все действия, с точки зрения их разрешения или запрета на исполнение пользователем, можно разделить на три категории:

- разграничиваемые;
- всегда разрешенные;
- всегда запрещенные.

Из разграничиваемых действий для каждого пользователя создается свой список разрешенных операций пользователя.

Решение о разрешении или запрете на исполнение разграничиваемых действий принимается на основе списка разрешенных пользователю операций и на основе меток, назначенных пользователю и всем объектам доступа, участвующим в операции. Кроме того, свое влияние оказывает также политика прокси-сервера.

Подробнее о процедурах настройки политики прокси-сервера, настройки меток, настройки разрешенных пользователю операций см. в соответствующих пунктах «Руководства по установке» (11443195.4012.069 98).

#### 4.2.6. Работа с группами

Любые объекты и субъекты могут быть объединены в группы – наборы элементов, для которых возможно одновременное назначение меток безопасности.

Использование групп позволяет ускорить процесс назначения меток безопасности, реализовать сегментирование ВИ более наглядным и понятным образом, а также упростить контроль за назначенными метками.

Подробнее о работе с группами см. пункт «Работа с группами» «Руководства по установке» (11443195.4012.069 98).

#### 4.2.7. Работа с шаблонами

Работа с шаблонами аналогична работе с другими типами объектов виртуальной инфраструктуры за тем исключением, что шаблон может быть конвертирован в виртуальную машину и обратно.

Подробнее о работе с шаблонами см. пункт «Работа с шаблонами» «Руководства по установке» (11443195.4012.069 98).

#### 4.2.8. Работа с отчетами

Отчеты позволяют увидеть, какие метки назначены объектам доступа и пользователям, а также обнаружить незарегистрированные объекты и пользователей, для которых не назначены ни уровни, ни категории.

Подробнее о работе с отчетами см. пункт «Работа с отчетами» «Руководства по установке» (11443195.4012.069 98).

### 4.3. Работа с сервисом регистрации событий

#### 4.3.1. Общие сведения

Если в инфраструктуре виртуализации предусмотрено наличие vCenter, сбор событий выполняется с vCenter и с ESXi. Если vCenter отсутствует, события собираются только с ESXi.

*Примечание: Причины возникающих неполадок в процессе работы сервиса регистрации событий «Сегмент-В.» выводятся также в стандартную утилиту просмотра событий операционной системы: Start -> Administrative tools -> Event Viewer.*

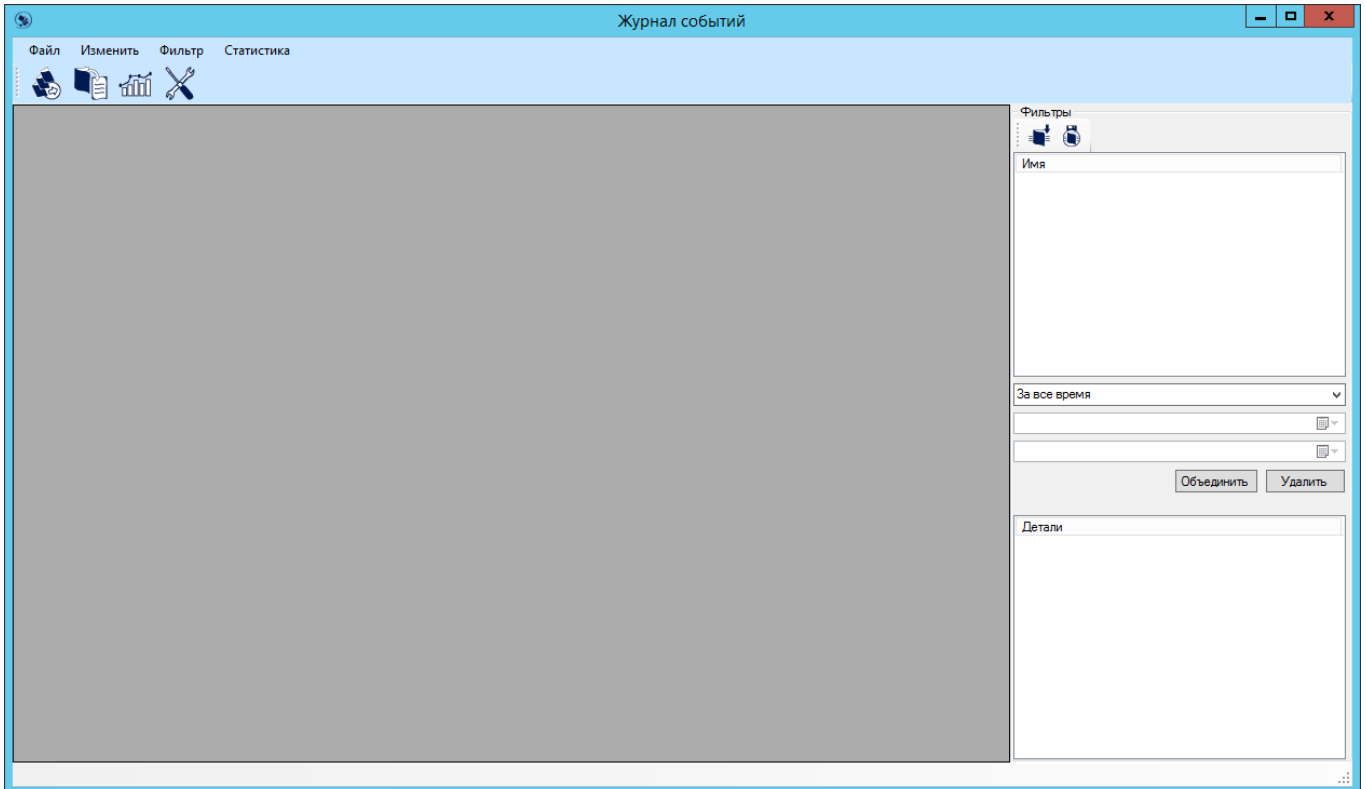
**ВНИМАНИЕ!** Файл конфигурации **Config.xml**, находящийся в корне папки с установленным сервисом регистрации событий, содержит список хостов и vCenter, с которых будут собираться события, и считывается только при запуске сервиса!

Если количество хостов и vCenter увеличилось или изменились их IP-адреса или имена, необходимо обновить данный конфигурационный файл (вручную или скопировав повторно с АРМ АБИ) и перезапустить сервис!

### 4.3.2. Получение событий

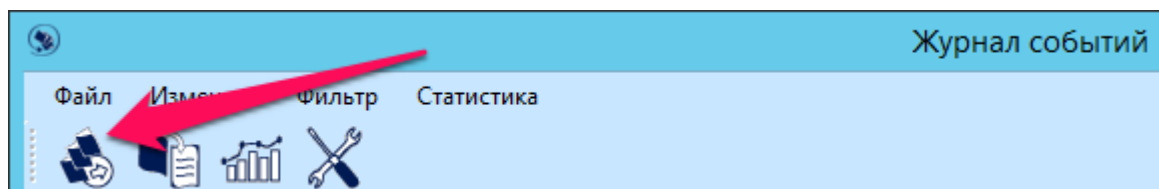
Для того чтобы начать работу с журналом регистрации событий, необходимо запустить с правами администратора утилиту «**LogViewer-V.**» на АРМ с установленным сервисом регистрации событий.

На экран выводится главное окно утилиты просмотра журнала регистрации событий (рисунок 3).



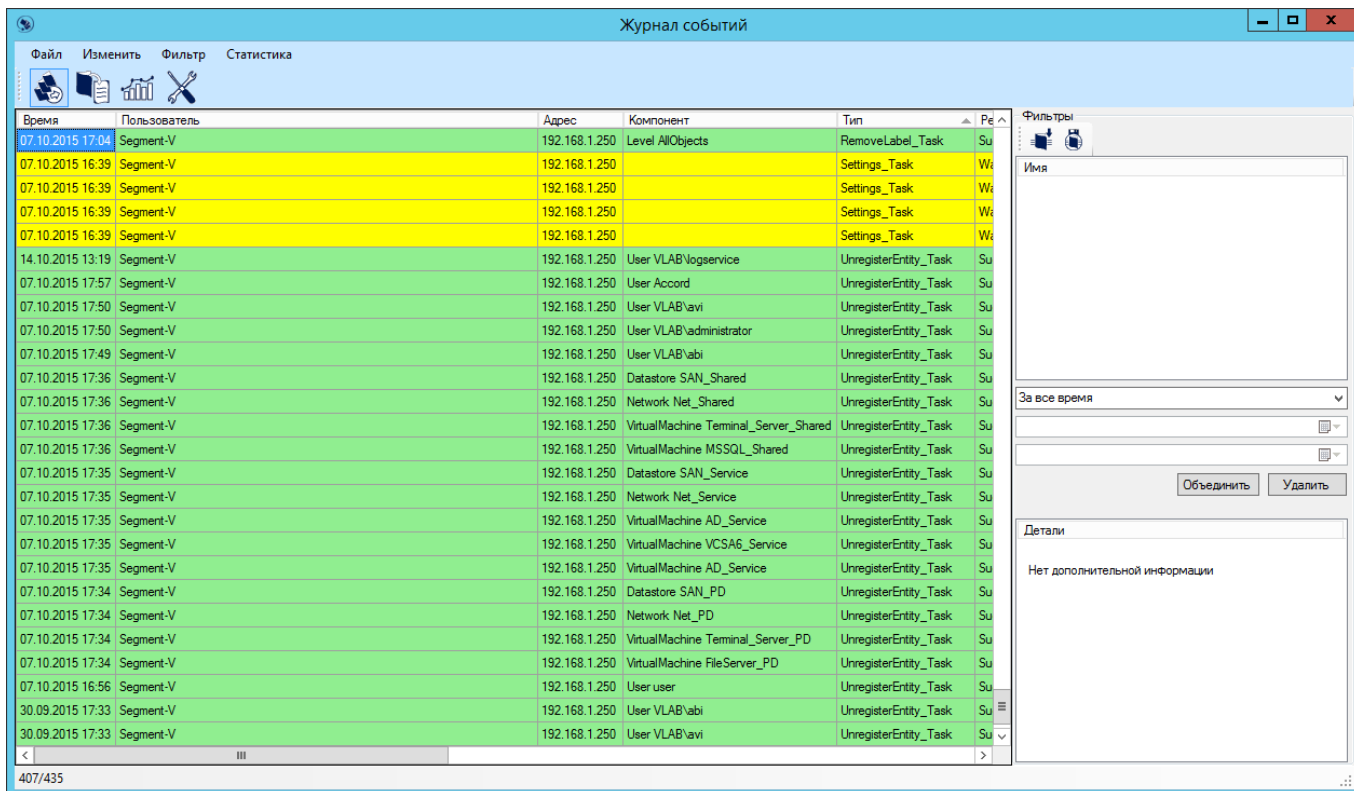
**Рисунок 3 - Главное окно утилиты просмотра зарегистрированных событий**

Для получения событий в главном окне журнала регистрации событий следует нажать кнопку <Получить события> (либо выбрать пункт меню «Файл»/ «Получить события» или нажать кнопку F5).



**Рисунок 4 – Кнопка <Получить события>**

На экран выводится список всех выполненных событий (рисунок 5).



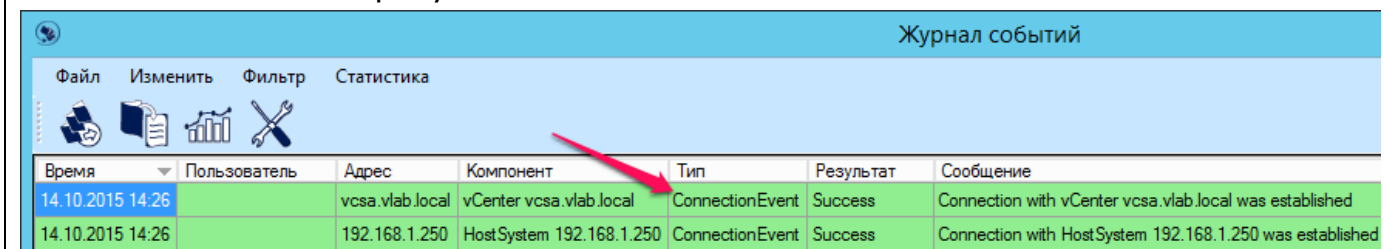
**Рисунок 5 – События в главном окне журнала**

**ВНИМАНИЕ!** События в журнале регистрации событий не обновляются автоматически – для получения актуальной информации необходимо выполнять процедуру их получения.

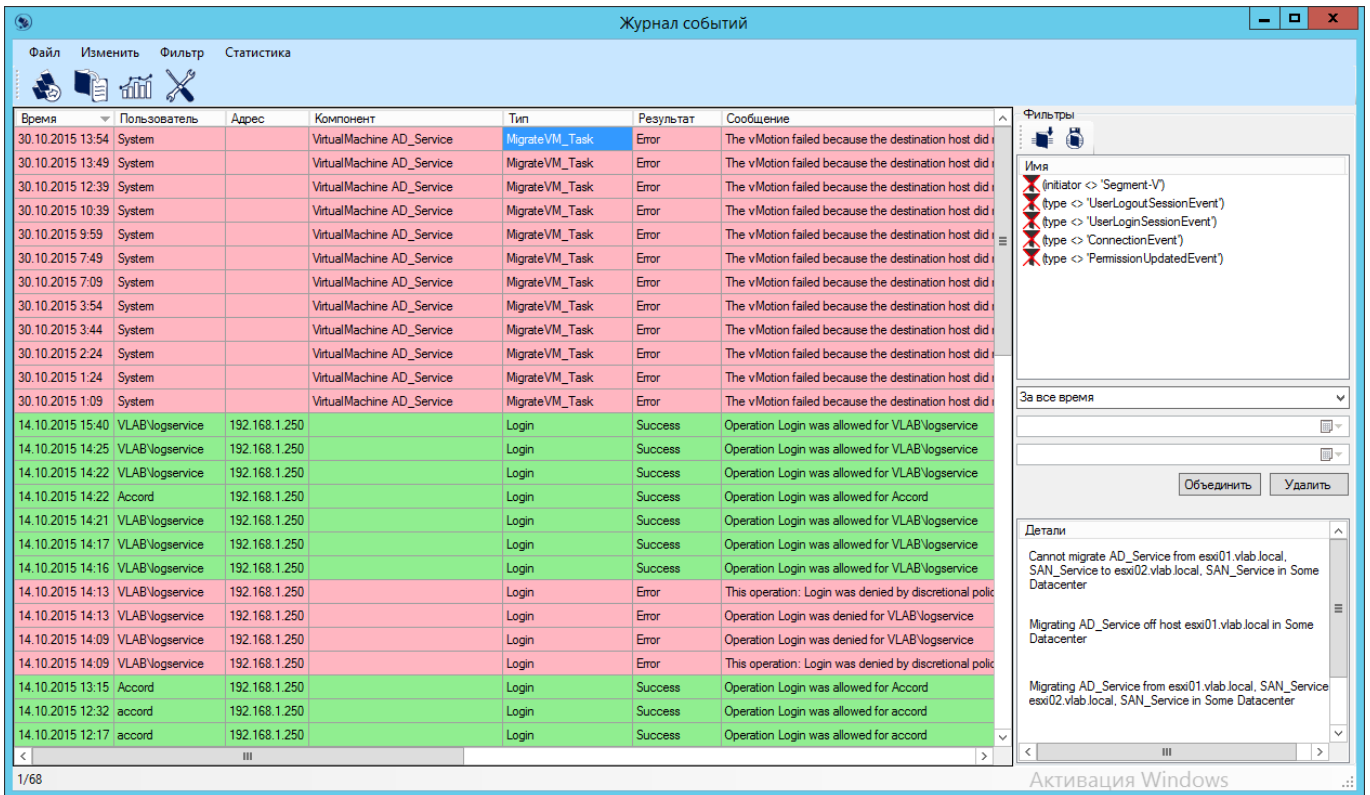
**ВНИМАНИЕ!** В списке полученных событий после первого старта сервиса отображаются события о подключении к vCenter и прокси-серверам «Сегмент-В.» (тип «ConnectionEvent» – показывает, что соединение с указанными в файле конфигурации элементами прошло успешно). Необходимо удостовериться, что события подключения существуют для всех заданных элементов (всех прокси-серверов и vCenter)!

Возможной причиной, по которой соединение может быть не установлено, является рассинхронизированное время (подробнее см. «Руководство по установке» (11443195.4012.069 98)).

В дальнейшем, если соединение потеряно, сгенерируется событие с типом «ConnectionEvent» и результатом «Error».



Для некоторых событий (например, для изменения конфигурации или неудачной миграции ВМ) доступно расширенное описание по двойному клику мыши (рисунок 6).



**Рисунок 6 – Главное окно журнала регистрации событий**

В этом случае следствием двойного щелчка мышью по выбранной строке является вывод на экран окна с подробным описанием события (рисунок 7).





```
-<Data>
-<VmFailedMigrateEvent>
  -<destHost>
    -<host>
      <type>HostSystem</type>
      <Value>host-37</Value>
    </host>
    <name>esxi02.vlab.local</name>
  </destHost>
  -<reason>
    -<fault>
      <reason>The vMotion failed because the destination host did not receive data from the source host on the vMotion network. Please check your vMotion network settings and physical network configuration and ensure they are correct.</reason>
    </fault>
  </reason>
  -<faultMessage>
    <key>msg.checkpoint.migration.nodata</key>
    <message>The vMotion failed because the destination host did not receive data from the source host on the vMotion network. Please check your vMotion network settings and physical network configuration and ensure they are correct.</message>
    <key>msg.vmotion.connect.failure</key>
    <message>The vMotion migrations failed because the ESX hosts were not able to connect over the vMotion network. Check the vMotion network settings and physical network configuration.</message>
    <key>vob.vmotion.net.send.connect.failed.status</key>
  </faultMessage>
  -<arg>
    <key>1</key>
    <value>167903845</value>
    <key>2</key>
    <value>1446198768010024</value>
    <key>3</key>
    <value>10.2.2.102</value>
    <key>4</key>
    <value>The ESX hosts failed to connect over the VMotion network</value>
    <Length>4</Length>
    <LongLength>4</LongLength>
    <Rank>1</Rank>
  </arg>
</VmFailedMigrateEvent>
</Data>
```

Рисунок 7 – Окно с расширенным описанием события

### 4.3.3. Работа с фильтрами

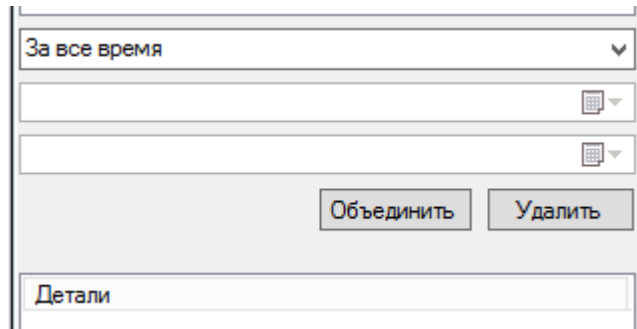
#### 4.3.3.1. Общие сведения

Для удобства, в процессе работы с журналом регистрации событий имеется возможность применения различных фильтров для выборки необходимых событий. Это возможно путем перетаскивания мышкой значений из таблицы в поле «Фильтры». Для применения установленных параметров фильтрации необходимо нажать кнопку <F5> или «Получить события».

В целом логика работы фильтров соответствует законам математической логики Де Моргана.

По умолчанию к фильтрам применяется логическое «И» (например: «инициатор root и IP = 192.168.53.53»).

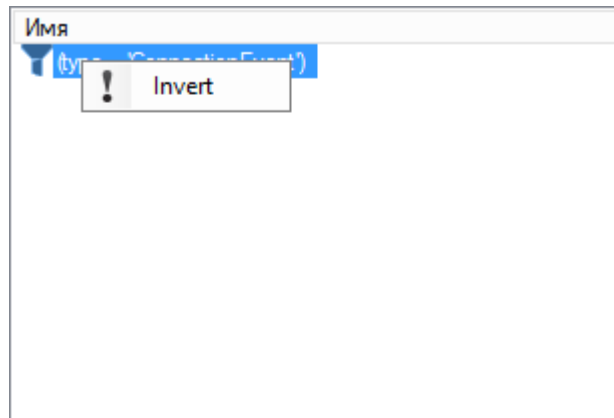
В случае использования кнопки «Объединить» (рисунок 8) к фильтрам применяется логическое «ИЛИ».



**Рисунок 8 - Кнопки <Объединить> и <Удалить>**

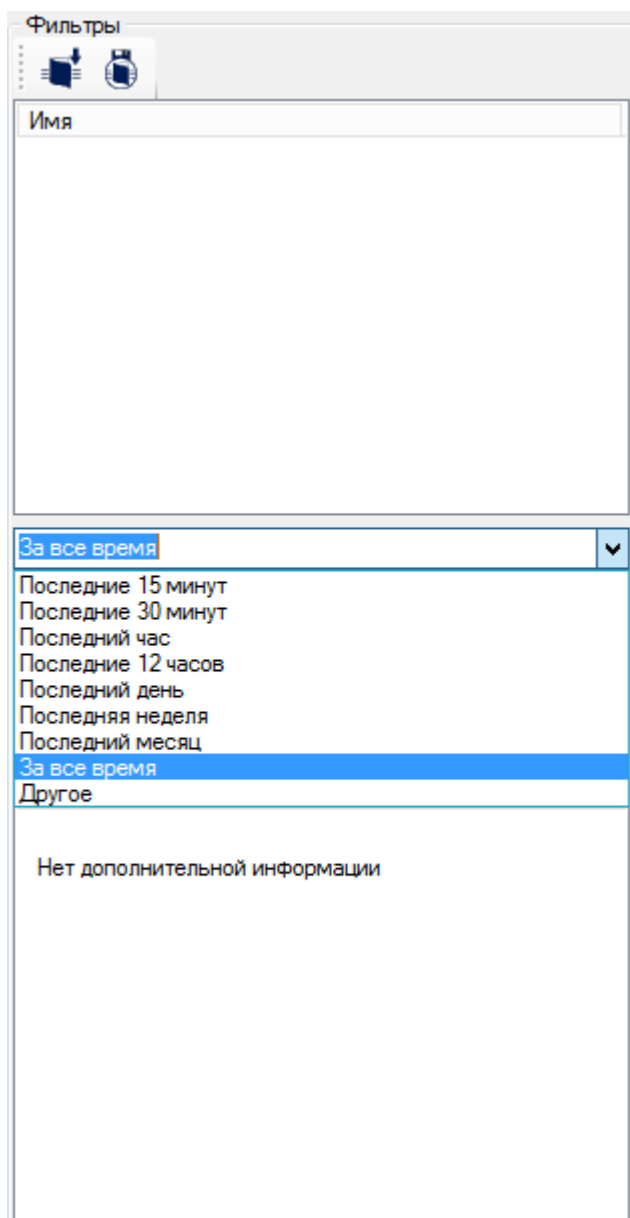
Для удаления какого-либо фильтра используется кнопка <Удалить> (рисунок 8).

При нажатии правой клавишей мыши на фильтр появляется возможность его инвертировать(рисунок 9).



**Рисунок 9 – Инвертирование фильтра**

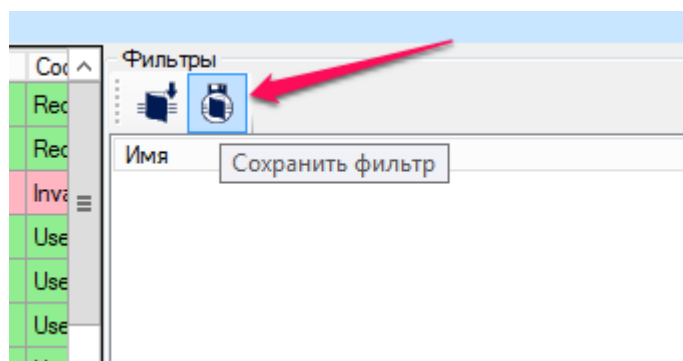
Имеется возможность фильтрации событий по времени (рисунок 10).



**Рисунок 10 - Фильтрация событий по времени**

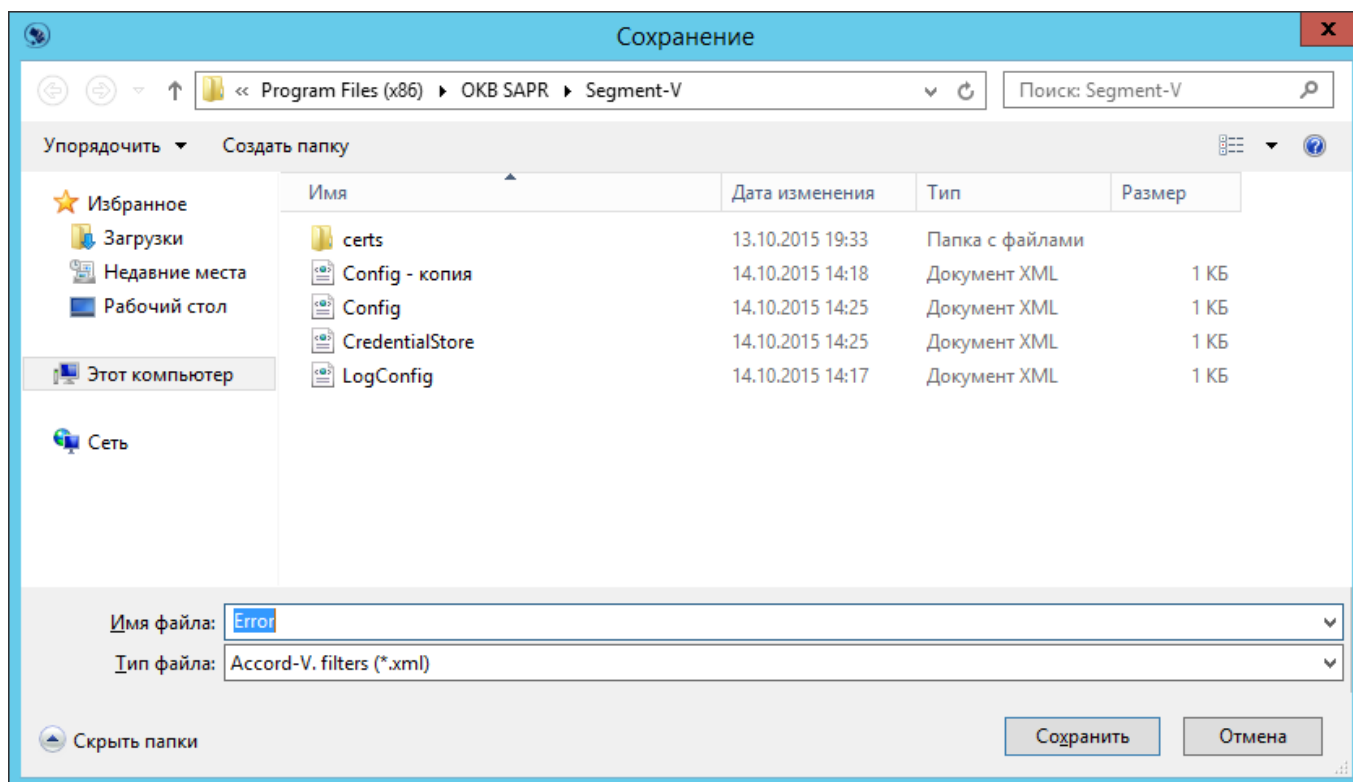
#### 4.3.3.2. Сохранение фильтра в файл

При необходимости фильтр можно сохранить в файл посредством нажатия кнопки <Сохранить фильтр> справа в окне журнала.



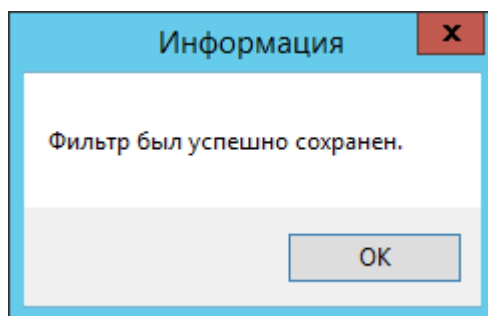
**Рисунок 11 - Кнопка <Сохранить фильтр>**

В появившемся далее окне следует выбрать нужный каталог для сохранения, задав при этом имя файлу, в который будет сохранен фильтр, и нажать кнопку <Save> (рисунок 12).



**Рисунок 12 – Сохранение фильтра**

В случае успешного выполнения описанной последовательности действий на экран выводится соответствующее сообщение (рисунок 13).

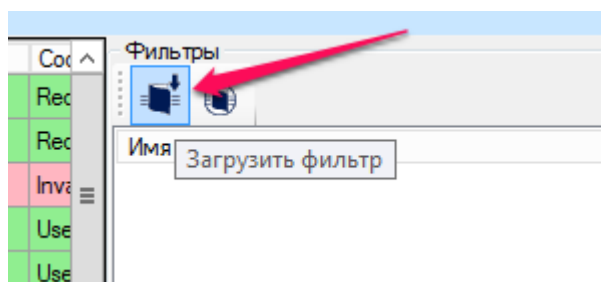


**Рисунок 13 – Сообщение об успешном сохранении фильтра**

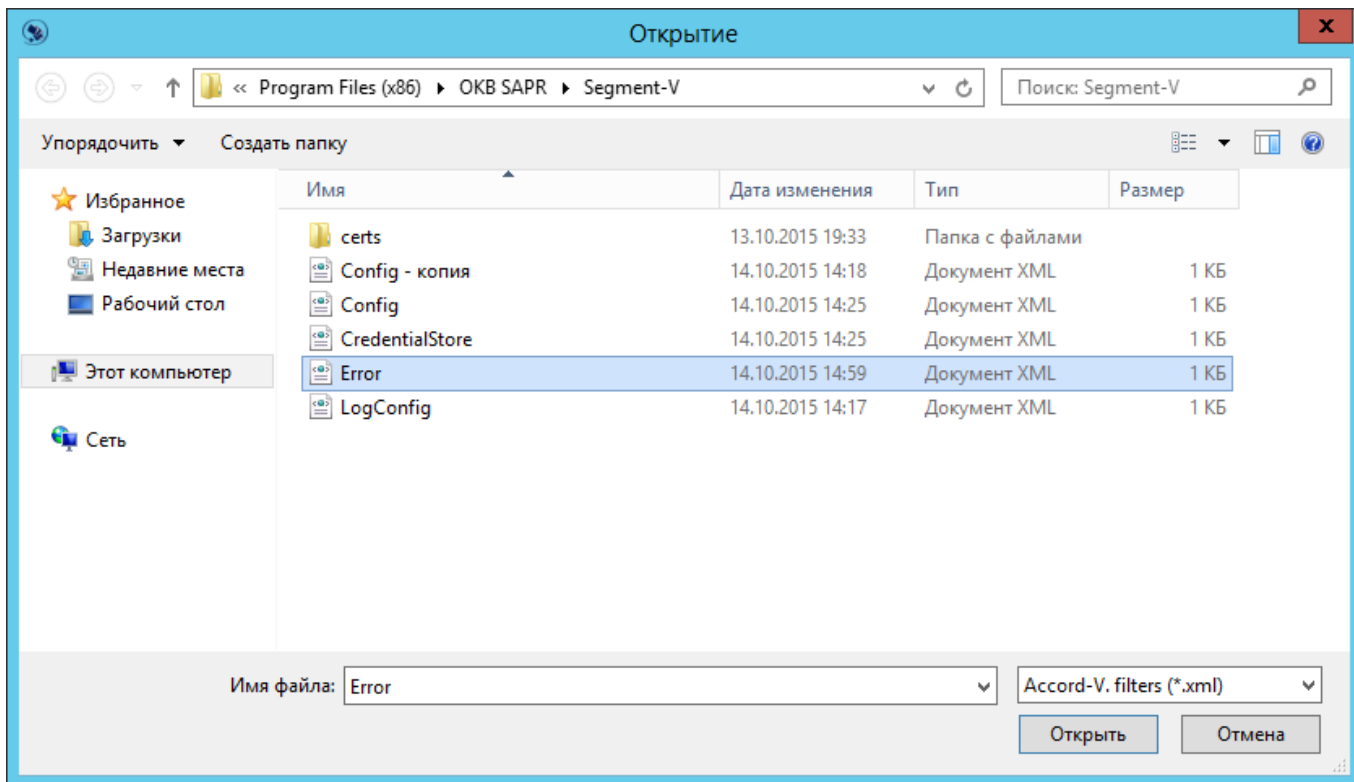
#### 4.3.3.3. Загрузка ранее сохраненного фильтра

Для того чтобы загрузить ранее сохраненный фильтр, следует нажать кнопку <Загрузить фильтр> и в появившемся окне выбрать нужный файл (рисунок 15).

**ВНИМАНИЕ!** При экспорте фильтров фильтр времени не экспортируется.

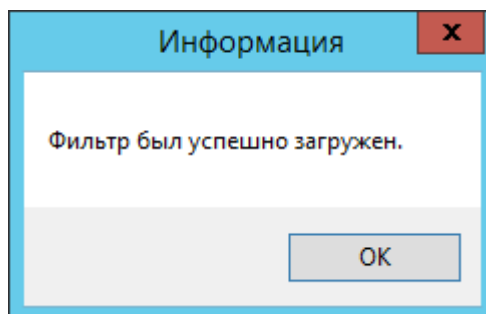


**Рисунок 14 - Кнопка <Загрузить фильтр>**



**Рисунок 15 – Загрузка ранее сохраненного фильтра**

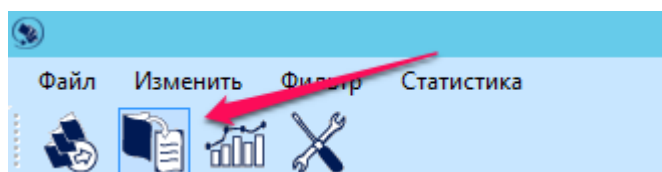
В случае успешного выполнения описанной последовательности действий на экран выводится соответствующее сообщение (рисунок 16).



**Рисунок 16 – Сообщение об успешной загрузке фильтра**

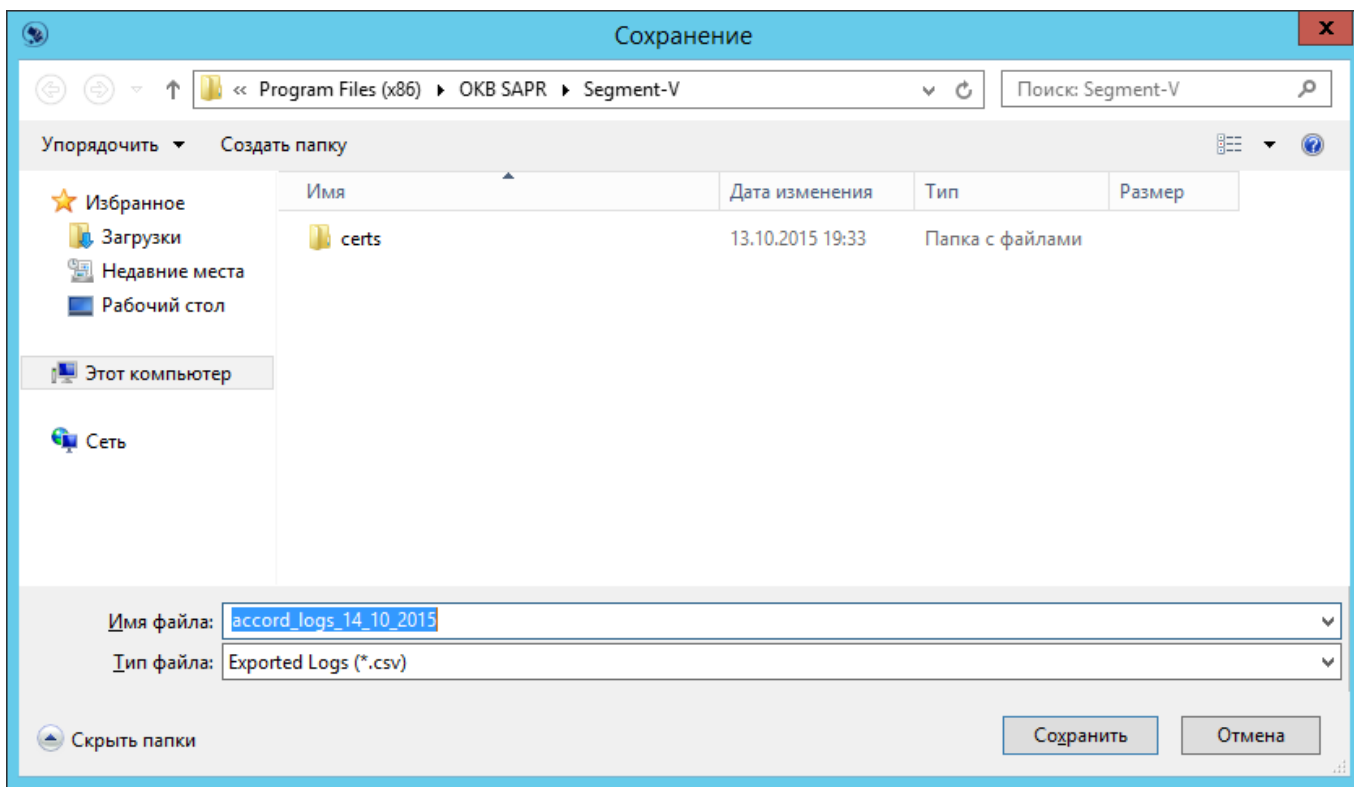
#### **4.3.4. Экспорт журнала**

Список полученных событий можно экспортировать (формат CSV) посредством нажатия кнопки <Экспортировать события в файл> (рисунок 17).



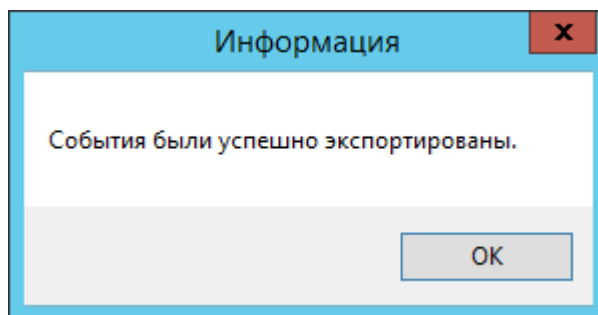
**Рисунок 17 – Кнопка <Экспортировать события в файл>**

В появившемся далее окне следует выбрать нужный каталог, задать название файлу, в который будут сохранены события, и нажать кнопку <Save> (рисунок 18).



**Рисунок 18 – Выбор каталога и задания имени файла для экспорта журнала**

В случае успешного выполнения описанной последовательности действий на экран выводится соответствующее сообщение (рисунок 19).

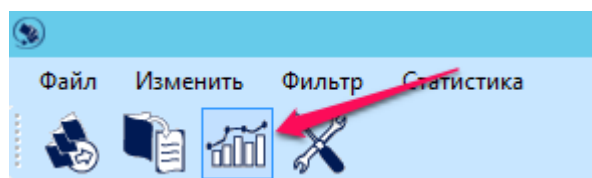


**Рисунок 19 – Сообщение об успешном выполнении процедуры экспорта журнала**

#### **4.3.5. Просмотр статистики по полученным событиям**

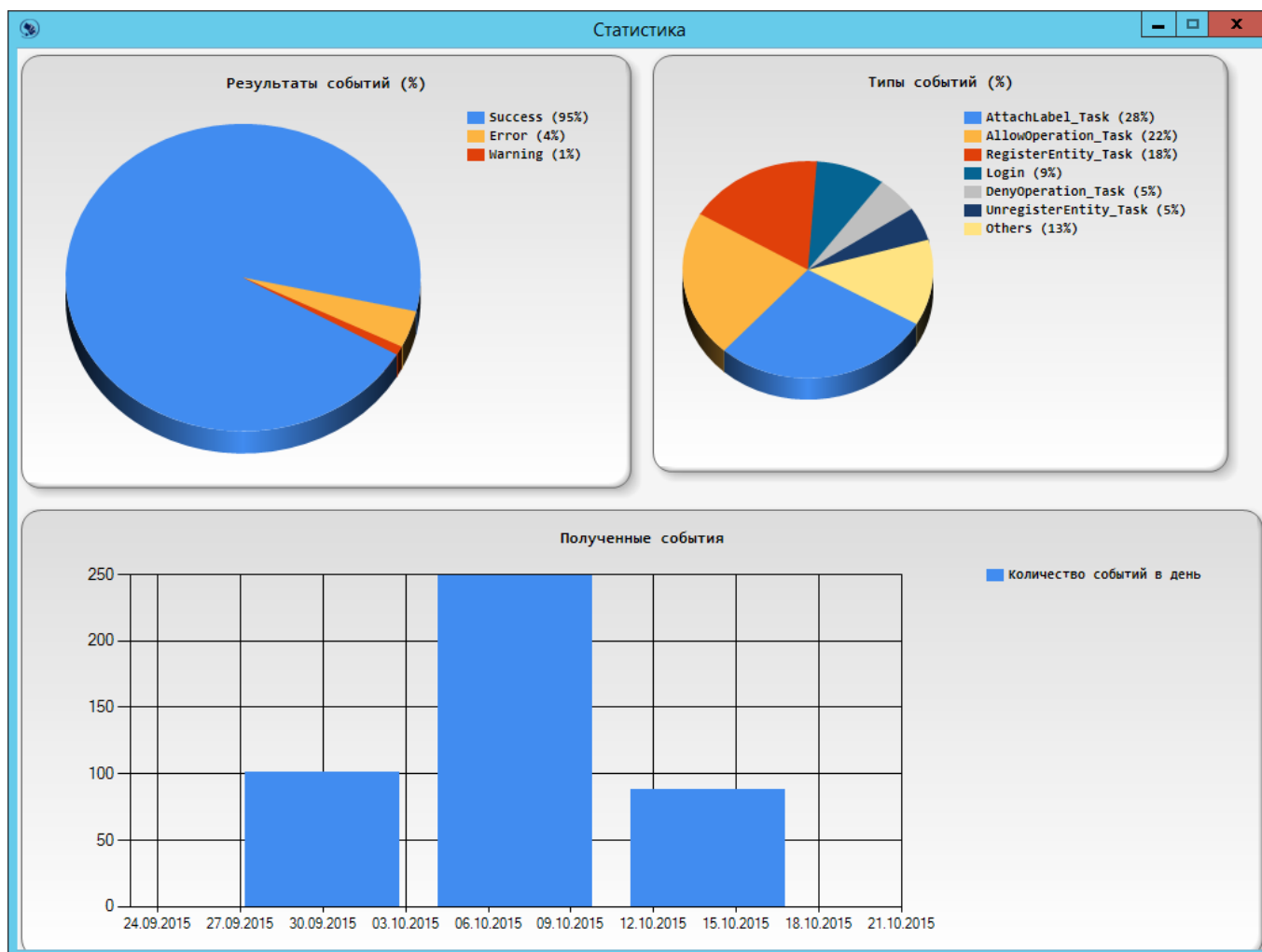
В утилите просмотра журнала регистрации событий предусмотрена возможность ведения статистики по полученным событиям.

Для этого следует в главном окне программы нажать кнопку <Анализ> (рисунок 20).



**Рисунок 20 - Кнопка <Анализ>**

В появившемся окне выводится статистика по количеству, типам и результатам полученных событий (рисунок 21).



**Рисунок 21 - Просмотр статистики**

#### 4.3.6. Настройки

Посредством нажатия кнопки <Настройки> (рисунок 22) имеется возможность настроить (рисунок 23):

- параметры цветовой схемы, используемой в утилите просмотра регистрируемых событий;
- IP-адрес и порт сервиса регистрации событий (данные параметры настраиваются администратором при первом сеансе работы – подробнее см. «Руководство по установке» (11443195.4012.069 98));



- максимальное количество событий, отображаемых в интерфейсе.

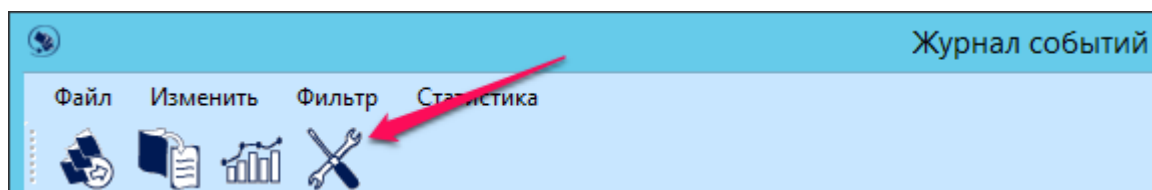


Рисунок 22 – Кнопка <Настройки>

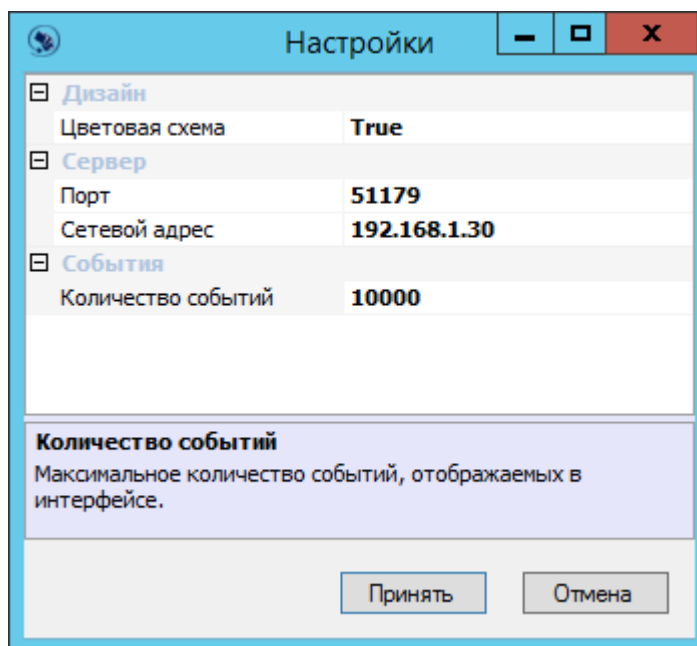


Рисунок 23 – Настройка IP-адреса сервиса регистрации событий

**ВНИМАНИЕ!** Ограничение в настройках на количество событий применяется к отображаемому количеству событий с учетом применения фильтра (т.е. по умолчанию 10 000 событий, попадающих под критерий заданного фильтра).

## 4.4. Работа с утилитой «Installer-V.»

### 4.4.1. Добавление серверов в список защищаемых

Процедура добавления серверов (ESXi/vCenter/прокси-серверы) в список защищаемых выполняется с помощью кнопки <Добавить сервер> в главном окне утилиты «**Installer-V.**» и подробно описана в п. «Настройка ПО управления» «Руководства по установке» (11443195.4012.069 98).

## 4.4.2. Работа с утилитой в случае совместного использования «Сегмент-В.» и «Аккорд-В.»

### 4.4.2.1. Установка агентов «Аккорд-В.» на ESXi

В случае совместного использования ПАК «Сегмент-В.» и ПАК «Аккорд-В.» установка агентов «Аккорд-В.» на ESXi производится централизованно с АРМ АБИ с помощью утилиты «**Installer-V.**», входящей в комплект поставки комплекса «Сегмент-В.».

Данная процедура выполняется аналогично процедуре установки агентов на ESXi с помощью утилиты «**Accord-V Installer**», входящей в комплект поставки ПАК «Аккорд-В.», и подробно описана в п. «Установка агентов «Аккорд-В.» на ESXi» в «Руководстве по установке» на комплекс «Аккорд-В.» (11443195.4012.028 98).

### 4.4.2.2. Регенерация сертификатов

Службы «Аккорд-В.» передают между собой информацию по протоколу SSL с использованием российской криптографии. В начале каждого соединения между ПО управления комплексом и всеми агентами «Аккорд-В.» на ESXi-серверах происходит двусторонняя идентификация и аутентификация, поэтому до начала взаимодействия соответствующие сертификаты и ключи, распределяются между всеми участниками информационного обмена.

В процессе установки агентов «Аккорд-В.» на ESXi распространение сертификатов на ESXi-серверы производится автоматически.

По умолчанию срок действия сертификатов составляет 365 дней (параметр `default_days` в файле `openssl.cfg`).

В случае необходимости, можно выполнить процедуру регенерации сертификатов при помощи утилиты «**Installer-V.**» (из комплекта поставки ПАК «Сегмент-В.»), в главном окне программы выбрав из списка нужный хост и нажав кнопку <Сгенерировать сертификаты>.

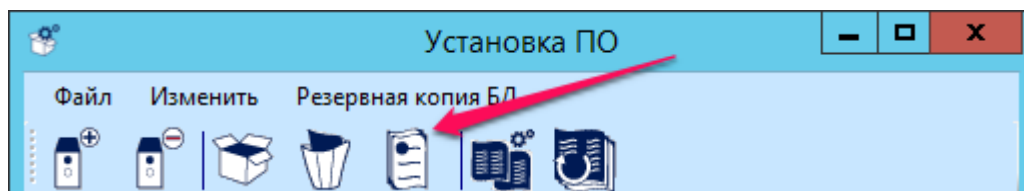


Рисунок 24 - Кнопка <Сертификаты>

Процедура регенерации сертификатов при помощи утилиты «**Installer-V.**» (из комплекта поставки ПАК «Сегмент-В.») выполняется аналогично процедуре установки агентов на ESXi с помощью утилиты «**Accord-V Installer**», входящей в комплект поставки ПАК «Аккорд-В.», и подробно описана в п. «Регенерация сертификатов» в «Руководстве администратора» на комплекс «Аккорд-В.» (11443195.4012.028 90).

### 4.4.3. Создание резервной копии и восстановление БД

Для создания резервной копии БД с ESXi следует в главном окне утилиты «Installer-V.» выбрать нужный ESXi и нажать кнопку <Создать резервную копию БД> (рисунок 25).

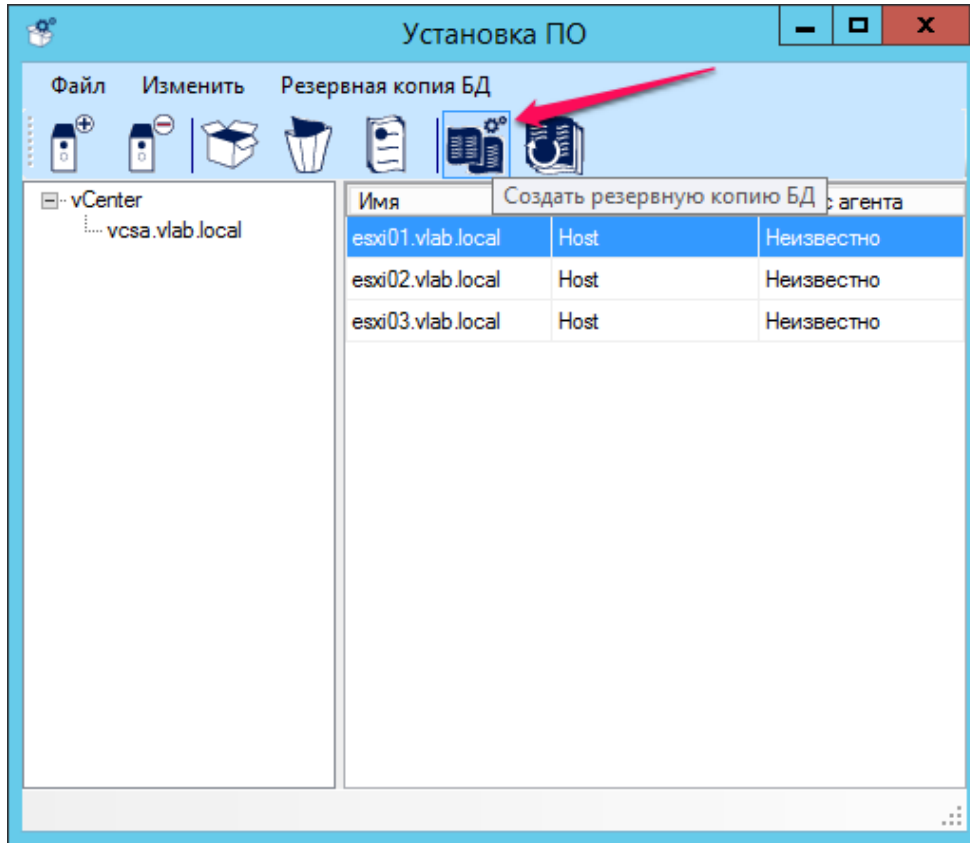
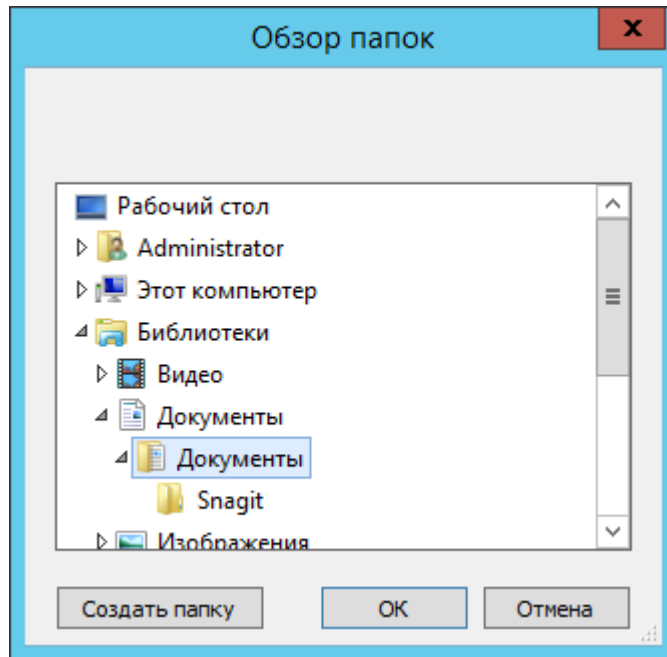


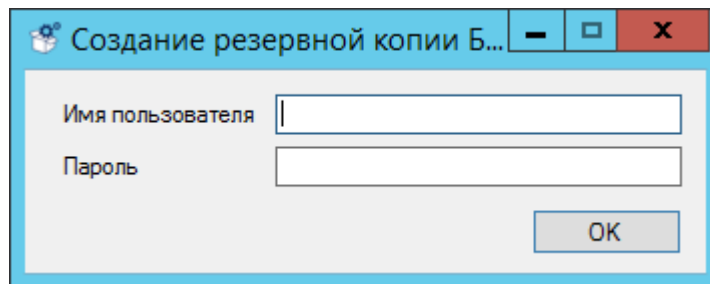
Рисунок 25 – Создание резервной копии БД

В появившемся далее окне следует указать путь к каталогу, в который будет помещена резервная копия БД, и нажать кнопку <ОК>.



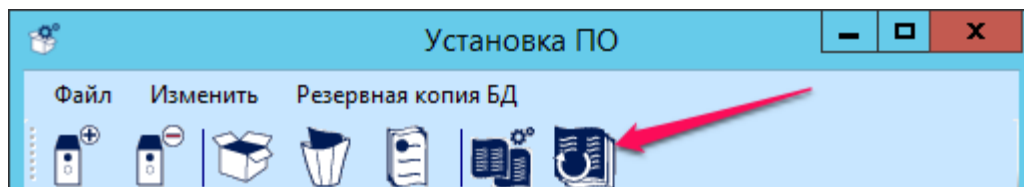
**Рисунок 26 - Выбор каталога для создания резервной копии БД**

В появившемся далее окне следует ввести имя и пароль учетной записи пользователя ESXi.



**Рисунок 27 - Ввод параметров учетной записи пользователя ESXi**

Для восстановления резервной копии БД с ESXi следует запустить утилиту «Installer-V.» и нажать кнопку <Восстановить БД из резервной копии> (рисунок 28).



**Рисунок 28 - Кнопка <Восстановить БД из резервной копии>**

В появившемся далее окне следует указать путь к резервной копии БД и нажать кнопку <ОК> (рисунок 29).

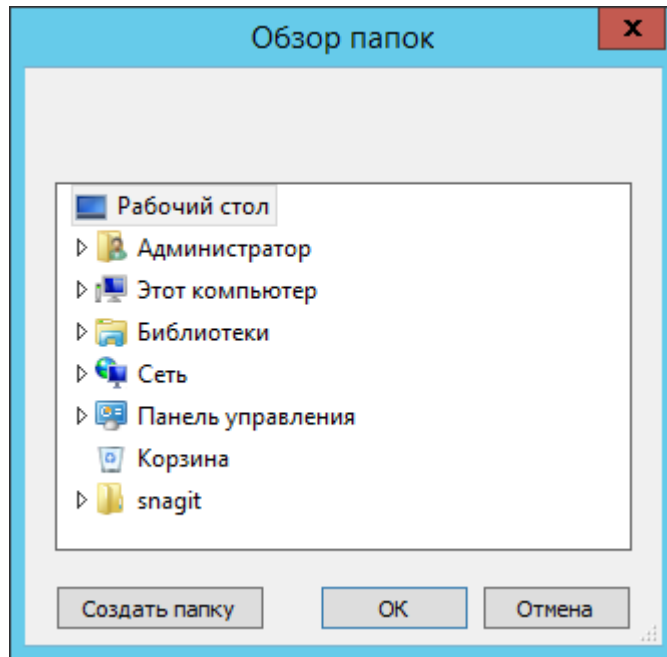


Рисунок 29 - Выбор каталога с резервной копией БД

## 5. Работа на клиентских рабочих местах

Работа на клиентских рабочих местах выполняется пользователем ПАК «Сегмент-В.» в соответствии с «Руководством пользователя» (11443195.4012.069 34).

**ВНИМАНИЕ!** Для выполнения процедур идентификации и аутентификации в виртуальной машине, которая находится в защищаемой инфраструктуре виртуализации, пользователю необходимо предъявлять персональный идентификатор; поэтому администратор безопасности информации должен настроить возможность проброса идентификатора пользователя с клиентского рабочего места в виртуальную машину.

## 6. Возможные затруднения в работе с ПАК «Сегмент-В.» и методы их устранения

Подробное описание см. в «Руководстве по установке» (11443195.4012.069 98), входящем в комплект поставки комплекса.

## 7. Техническая поддержка и информация о комплексе

Все вопросы, связанные с поддержкой ПАК «Сегмент-В.», Вы можете отправлять по адресу [help@okbsapr.ru](mailto:help@okbsapr.ru), либо обращаться по телефонам +7 (499) 235-78-17, +7 (926) 235-89-17, +7 (926) 762-17-72.

Мы будем рады узнать Ваши пожелания и предложения по поводу этой документации. Вы можете отправить их по адресу [help@okbsapr.ru](mailto:help@okbsapr.ru).