

# ЦУГИ: Система мониторинга инфраструктуры открытых ключей

Руководство администратора

20.12.2021

## Содержание

|       |  |    |
|-------|--|----|
| 1     | Введение .....   | 4  |
| 1.1   | Наименование программного изделия .....                            | 4  |
| 1.2   | Перечень сокращений и терминов .....                               | 4  |
| 2     | Общие положения .....  | 5  |
| 2.1   | Назначение документа .....   | 5  |
| 2.2   | Соглашения и обозначения .....                                     | 5  |
| 3     | Назначение программного изделия .....                              | 6  |
| 3.1   | Основные возможности .....   | 6  |
| 3.2   | Архитектура .....  | 7  |
| 4     | Установка .....  | 8  |
| 4.1   | Общие положения .....  | 8  |
| 4.2   | Состав дистрибутива .....  | 8  |
| 4.3   | Требования к Серверам и рабочим местам .....                       | 9  |
| 4.3.1 | Требования к серверу программного компонента Сервер ЦУГИ .....     | 9  |
| 4.3.2 | Требования к системе виртуализации .....                           | 9  |
| 4.3.3 | Требование к рабочим местам .....                                  | 10 |
| 4.3.4 | Требования к сети передачи данных .....                            | 10 |
| 4.4   | Установка обеспечивающих программ .....                            | 10 |
| 4.5   | Настройка взаимодействия с доменом Active Directory .....          | 10 |
| 4.6   | Технологические учётные записи для работы ЦУГИ .....               | 11 |
| 4.7   | Установка серверного компонента ЦУГИ .....                         | 11 |
| 4.7.1 | Последовательность установки .....                                 | 12 |
| 4.7.2 | Проверка установки .....   | 16 |
| 4.8   | Удаление Сервера ЦУГИ .....  | 16 |
| 5     | Настройка системы .....  | 18 |
| 5.1   | Настройки ЦУГИ для работы в сетевой конфигурации .....             | 18 |
| 5.2   | Настройка подключения системы ЦУГИ к домену Active Directory ..... | 25 |
| 5.3   | Настройка мониторинга компонентов Сервера .....                    | 28 |
| 5.4   | Настройка мониторинга компонентов ИОК .....                        | 30 |
| 5.5   | Настройка диаграмм .....   | 30 |
| 5.6   | Настройка функции «Сертификаты с ЦС» .....                         | 33 |
| 5.7   | Настройка «Сертификаты с серверов» .....                           | 33 |

|       |  |    |
|-------|--|----|
| 5.7.1 | Оповещения об истекающих сертификатах с серверов ..... | 35 |
| 5.8   | Настройка «Шаблоны» .....                              | 35 |
| 5.9   | Настройка функции «Сводная таблица» .....              | 35 |
| 5.10  | Настройка функции «ИОК резервное копирование» .....    | 36 |
| 5.11  | Настройка функции «Запросы» сертификатов .....         | 36 |
| 5.12  | Предоставление доступа .....                           | 37 |
| 6     | Аварийные ситуации .....                               | 38 |
| 6.1   | Резервное копирование ЦУГИ .....                       | 38 |
| 6.2   | Восстановление системы из резервной копии ЦУГИ.....    | 38 |

# 1 Введение

## 1.1 Наименование программного изделия

Наименование — ЦУГИ: Система мониторинга инфраструктуры открытых ключей.

Шифр программного изделия — «ЦУГИ».

Обозначение программного изделия — 69639709.СП0411.001.

## 1.2 Перечень сокращений и терминов

ЦУГИ — сокращённое наименование и шифр разработки программного изделия «Система централизованного анализа и управления гетерогенными инфраструктурами».

ITC Portal — англоязычное наименование программного изделия «Система централизованного анализа и управления гетерогенными инфраструктурами».

ИОК — Инфраструктура открытых ключей (ИОК, англ. PKI — Public Key Infrastructure) — набор средств (технических, материальных, людских и т. д.), распределённых служб и компонентов, в совокупности используемых для поддержки задач криптографической защиты информации на основе закрытого и открытого ключей.

ВМ — Виртуальная машина.

ОЗУ — Оперативное запоминающее устройство.

ОС — Операционная система.

ПО — Программное обеспечение.

СУБД — Система управления базами данных.

ЦПУ — Центральное процессорное устройство, процессор сервера.

ЦС — Центр сертификации.

IIS — Диспетчер сервера приложений (Internet Information Server).

SQL — Structured Query Language — язык программирования, применяемый для создания, модификации и управления данными в реляционной базе данных, под управлением соответствующей системы (СУБД).

## 2 Общие положения

### 2.1 Назначение документа

Руководство предназначено для лиц, осуществляющих установку, настройку и сопровождение программного обеспечения системы ЦУГИ.

Руководство содержит описание действий по установке, настройке, удалению программного изделия, а также описание базовых операций по управлению системой ЦУГИ и диагностированию возможных неисправностей.

Руководство не заменяет учебную, справочную литературу, документацию производителя операционной системы и прочие источники информации, описывающие работу операционной системой, системы управления базой данных, их графических интерфейсов.

### 2.2 Соглашения и обозначения

| Формат            | Значение   |
|-------------------|--|
| Обычный           | Основной текст инструкции  |
| Полужирный        | Применяется для написания наименований заголовков окон и вкладок в них, имён команд, названий модулей и программных компонентов, кнопок и других управляющих элементов окон (переключателей, селекторных кнопок), а также наименований полей ввода, раскрывающихся списков и других информационных элементов интерфейса. |
| Полужирный курсив | Применяется для написания наименований папок, файлов различного типа и путей доступа к ним.  |

Словосочетание «щелчок мышью» применяется для обозначения однократного, а «двойной щелчок» – быстрого двукратного нажатия на левую кнопку манипулятора типа «мышь».

Словосочетание «нажать кнопку (или нажать на кнопку)» означает: «навести указатель мыши на кнопку, и выполнить щелчок мышью».

## 3 Назначение программного изделия

Программное изделие ЦУГИ предназначено для решения следующих задач:

- Мониторинга состояния компонентов ИОК в гетерогенных инфраструктурах;
- Автоматизации и централизации управления сертификатами в различных ЦС, входящих в ИОК;
- Снижения нагрузки на администраторов ИОК за счет реализации самообслуживания пользователей.

### 3.1 Основные возможности

- Представление сводной информации по всем компонентам на едином экране или в виде многоуровневой структуры.
- Настраиваемое графическое отображение состояния и счетчиков производительности серверов ИОК в виде диаграмм и статусов.
- Уведомления при наступлении критического события.
- Поиск данных о сертификатах из различных ЦС (инвентаризация сертификатов).
- Индивидуальные настройки оповещений об истекающих сертификатах.
- Интеграция с разнообразными средствами управления сертификатами, компонентами ИОК и смежными системами.
- Возможность мониторинга инфраструктуры ИОК на базе алгоритмов шифрования ГОСТ.
- Представление сводной информации по всем компонентам на едином экране.
- Мониторинг изменения шаблонов сертификатов и состава опубликованных шаблонов.
- Мониторинг и выполнение резервной копии ЦС.
- Возможность настройки различного типа оповещений через электронную почту.
- Возможность запроса сертификатов.
- Адаптивный интерфейс для использования на различных устройствах.

## 3.2 Архитектура

На рисунке ниже представлена Архитектура системы, сосредоточенная на бизнес-логике для мониторинга инфраструктуры открытых ключей. Эта логика и специальная функциональность достигается наличием в составе системы модуля мониторинга ИОК. Другие компоненты ЦУГИ являются базовыми для образования большинства версий функциональности Системы.

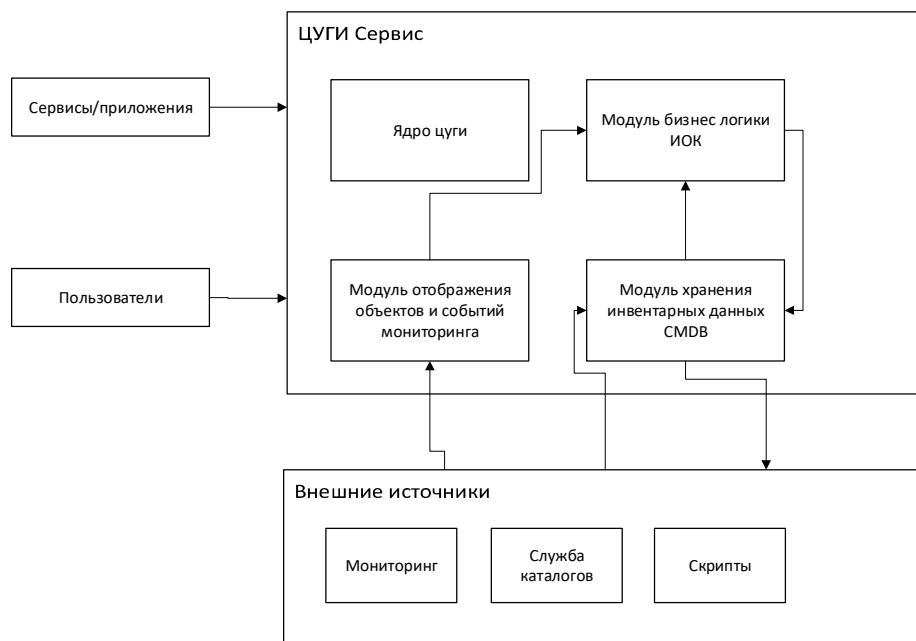


Рисунок 1 – Схема архитектуры системы ЦУГИ.

## 4 Установка

Примечание — Для установки и настройки серверов ЦУГИ рекомендуется обратиться в организацию разработчика.

### 4.1 Общие положения

Загружаемая версия ЦУГИ по умолчанию настроена для работы в односерверной конфигурации. Конфигурация по умолчанию позволяет выполнять задачи инвентаризации сертификатов, сбора и графического отображения счетчиков производительности, настройки отображения сводной информации, и управления заданиями только для сервера, на котором установлена система.

Допускается самостоятельное расширение односерверной конфигурации для выполнения задач инвентаризации сертификатов и мониторинга производительности дополнительных серверов в сети, при условии настройки системы ЦУГИ для использования доступного в сети доменного имени (fqdn, fully qualified domain name) и выпуска для данного доменного имени сертификата таким образом, что для соответствующих серверов в сети установлены доверительные отношения с ЦС, выпустившим сертификат. Такая конфигурация ЦУГИ далее называется *сетевой конфигурацией*.

В случае сетевой конфигурации ЦУГИ необходима дополнительная настройка диспетчера сервера приложений IIS для использования сервисных учетных записей в домене Active Directory, и подключение системы ЦУГИ к домену Active Directory.

**Важно** - подключение системы ЦУГИ к различным реализациям ЦС (ГОСТ, Microsoft Active Directory Certificate Services и т. п.) для решения задач мониторинга ЦС, создания резервных копий ЦС, сбора и мониторинга изменений сертификатов и оповещения об истечении срока действия сертификатов выполняется специалистами организации разработчика.

### 4.2 Состав дистрибутива

Для установки ЦУГИ предоставляется дистрибутив-установщик с названием вида «setup\_2.0.0.msi» (цифры означают версию сборки ПО и могут отличаться от указанных в документации):

Дистрибутив-установщик можно записать на usb-носитель (требуется не менее 100 МБ свободного места), CD, или скачать на персональный компьютер с веб-сайта организации-разработчика (поставщика) при соответствующей авторизации пользователя.



## 4.3 Требования к Серверам и рабочим местам

### 4.3.1 Требования к серверу программного компонента Сервер ЦУГИ

По умолчанию система ЦУГИ устанавливается и автоматически настраивается для работы в односерверной конфигурации.

Системные требования для сервера ЦУГИ:

- ОС Windows Server Standard 2016 (сервер с графическим интерфейсом) или более поздняя;
- Язык ОС – Русский;
- 2 ядра;
- Оперативная память 8 ГБ;
- 100 ГБ дискового пространства;
- Сетевой адаптер 1 Гбит/с включенным протоколом TCP/IPv4.

Примечание — Описание установки Windows Server приведено на сайте Microsoft.

Для хранения данных система использует и автоматически устанавливает на целевой сервер СУБД PostgreSQL версии 13.

При больших объемах данных, инвентаризации и мониторинга рекомендуется использование СУБД PostgreSQL 12 версии 12 или выше на выделенном сервере. Для обеспечения высокого уровня доступности системы рекомендуется кластерная установка СУБД PostgreSQL. Настройка системы ЦУГИ для использования выделенного сервера СУБД выполняется специалистами организации разработчика.

### 4.3.2 Требования к системе виртуализации

Все компоненты ЦУГИ можно развернуть на виртуальных машинах при выполнении следующих требований:

- Производитель решения по виртуализации поддерживает в качестве гостевых операционных систем версии Windows Server, которые задействованы в разворачивании ЦУГИ и вспомогательных сервисов;
- Система виртуализации обладает ресурсами, необходимыми для развертывания ЦУГИ и вспомогательных сервисов;
- Выполняются требования по взаимному сетевому доступу ЦУГИ и вспомогательных сервисов.

#### 4.3.3 Требование к рабочим местам

Подключение к portalу ЦУГИ осуществляется при помощи браузера. Версии браузеров, поддерживающие подключение к portalу ЦУГИ:

- Microsoft Edge;
- Internet Explorer 11;
- Google Chrome 75.0.3770.100 и выше;
- Opera 60.0.3255.56 и выше;
- Firefox 67.0.4 и выше.

#### 4.3.4 Требования к сети передачи данных

Сервер ЦУГИ, сервер баз данных ЦУГИ, рабочие места с которых осуществляется доступ к ЦУГИ должны быть взаимно доступны по сети, т. е. находиться в одном широковещательном домене (в одной плоской сети) либо должна быть настроена маршрутизация на уровне L3.

Взаимодействие между компонентами системы и порталом ЦУГИ осуществляется по протоколу https с использованием порта 443. На целевом сервере ЦУГИ не должно быть установлено других веб-приложений, использующих порт 443. При нарушении этого требования корректная работа системы невозможна!

Примечание - при установке ЦУГИ в односерверной конфигурации доступ к portalу возможен только с целевого сервера по адресу <https://localhost>

В случае установки базы данных на выделенном сервере, ЦУГИ взаимодействует с сервером баз данных по протоколу TCP порт 5432.

### 4.4 Установка обеспечивающих программ

Все необходимые для функционирования ЦУГИ компоненты, включая дистрибутив PostgreSQL версии 13, входят в состав дистрибутива и устанавливаются автоматически. Необходимые роли и компоненты Windows Server активируются автоматически в процессе установки.

### 4.5 Настройка взаимодействия с доменом Active Directory

Для использования полного функционала ЦУГИ система должна быть настроена для работы с доменными технологическими учетными записями, а все компьютеры системы должны быть включены в один домен Active Directory, со следующими параметрами:

- версии контролеров домена не ниже Windows Server 2012 R2;

- уровень леса и домена не ниже Windows Server 2012 R2.

Для функционирования ЦУГИ в домене Active Directory, необходимо установить модуль Active Directory для Windows PowerShell. Установку можно осуществить при помощи команды PowerShell *Add-WindowsFeature -Name "RSAT-AD-PowerShell" -IncludeAllSubFeature*.

Установку модуля должен производить пользователь, обладающий на данном компьютере правами администратора операционной системы.

Для взаимодействия с доменом Active Directory система ЦУГИ использует учетные данные, от имени которых запускаются пулы приложений IIS (см. раздел 4.6).

## 4.6 Технологические учётные записи для работы ЦУГИ

В процессе установки ЦУГИ автоматически формируются локальные технологические учетные записи Windows, область применения которых ограничена конкретным компьютером, на котором установлена система.

Создаются следующие локальные технологические учетные записи:

| Объект         | Имя            | Назначение  |
|----------------|----------------|---|
| Учетная запись | itc            | Учетная запись для запуска пулов приложений IIS (ApplicationPool) |
| Учетная запись | Itcintegration | Учетная запись для импорта данных в ЦУГИ                          |

При настройке ЦУГИ для работы в домене, доменные технологические учетные записи также должны называться itc и itcintegration.

Программный компонент Сервер ЦУГИ при установке требует знания имени и пароля доменной учётной записи пользователя, обладающего правами локального администратора Windows, под которым был осуществлен вход в сеанс операционной системы или ввода их, если установщик был запущен не с повышенными привилегиями;

## 4.7 Установка серверного компонента ЦУГИ

Программные компоненты или комплексы, входящие в состав специального программного обеспечения системы ЦУГИ, должны устанавливаться на компьютеры, удовлетворяющие требованиям, изложенным в разделе 4.3.

ЦУГИ устанавливается на серверное оборудование (целевой сервер), которое будет входить в состав системы ЦУГИ. Установку должен производить пользователь, с использованием локальной или доменной учётной записи, которая

должна обладать на данном компьютере правами локального администратора операционной системы Windows.

Рекомендуется выполнять установку на ОС Windows Server 2016 Rus или Windows Server 2019 Rus, с установленными компонентами по умолчанию, без установки и настройки дополнительных ролей, компонентов и ПО. В процессе установки ЦУГИ автоматически устанавливает и настраивает все необходимые компоненты для функционирования портала ЦУГИ.

Компоненты ЦУГИ автоматически и безальтернативно устанавливаются в папку C:\inetpub\App на целевом сервере.

Важно - При наличии на целевом сервере сайта IIS, настроенного для работы с другим веб-приложением, корректная работа ЦУГИ невозможна!

#### 4.7.1 Последовательность установки

Для ЦУГИ установки необходимо выполнить файл Setup\_2.0.0.msi. После запуска установщика появляется следующее окно:

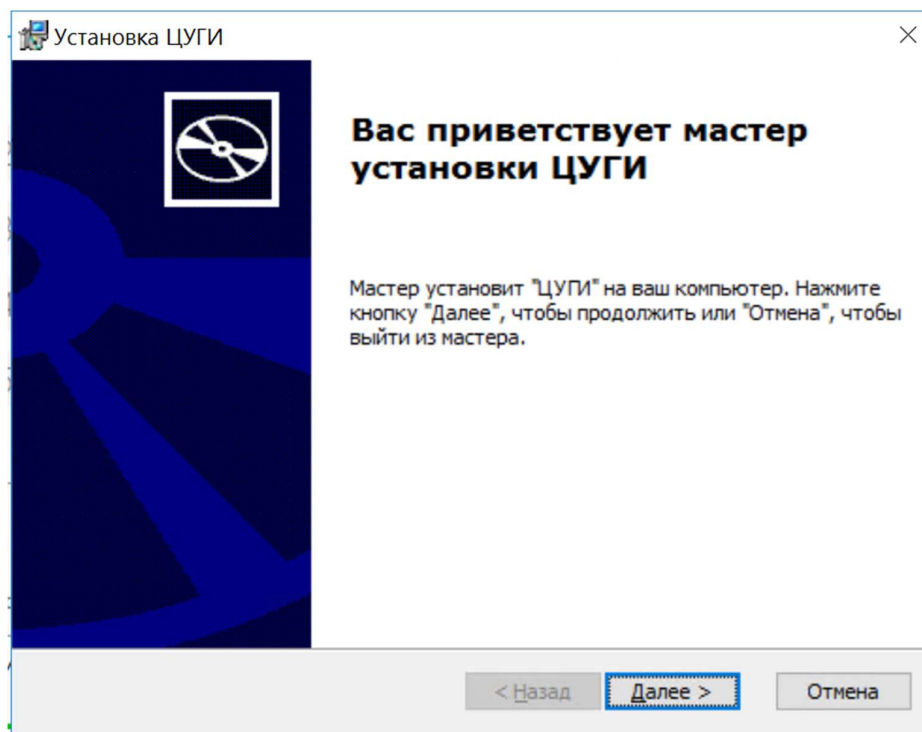


Рисунок 2 – Окно программы-установщика.

Для начала процесса установки необходимо нажать кнопку Далее, после чего появится окно с предложением ознакомиться и принять условия лицензионного соглашения ЦУГИ. При отказе принять условия, процесс установки завершается.

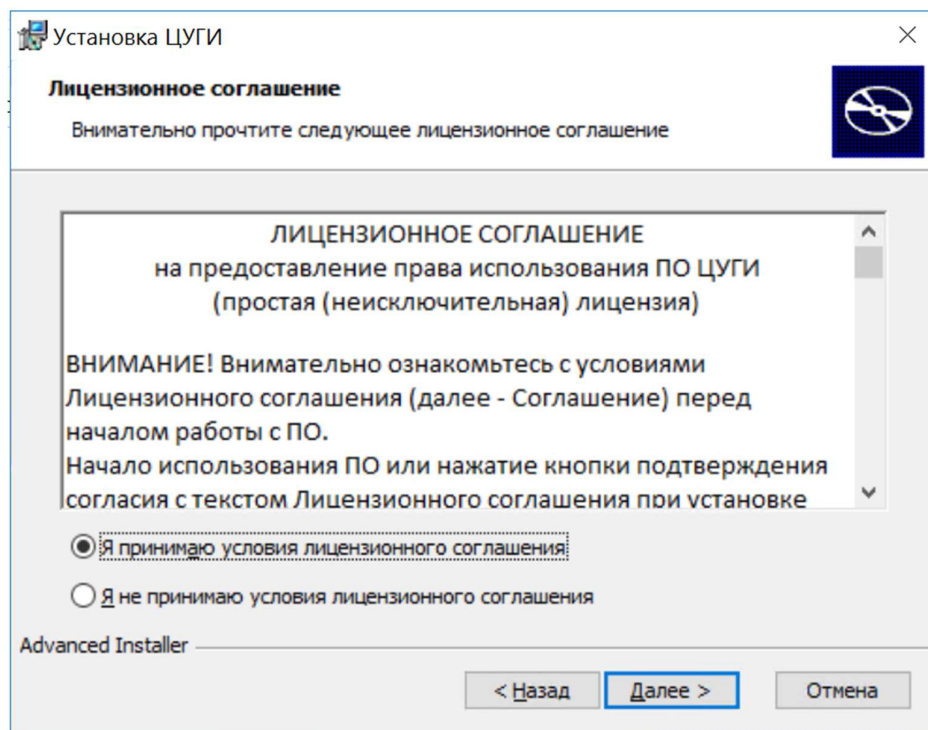


Рисунок 3 – Просмотр и принятие условий лицензионного соглашения.

После нажатия кнопки «Далее» появляется окно с предложением начать установку. При нажатии кнопки Установить процесс начинается. Устанавливается система ЦУГИ и компоненты, необходимые для ее работы, в том числе СУБД PostgreSQL 13.

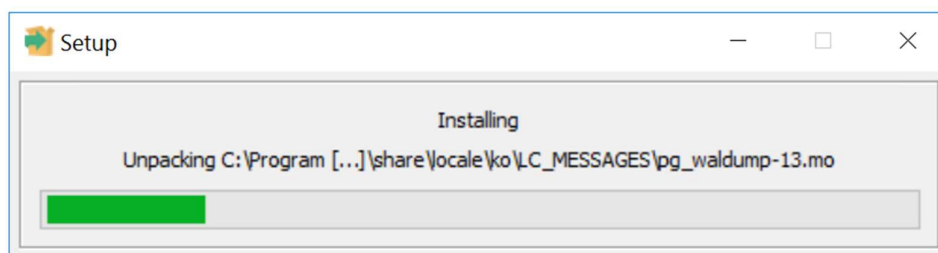


Рисунок 4 – Процесс установки СУБД PostgreSQL 13.

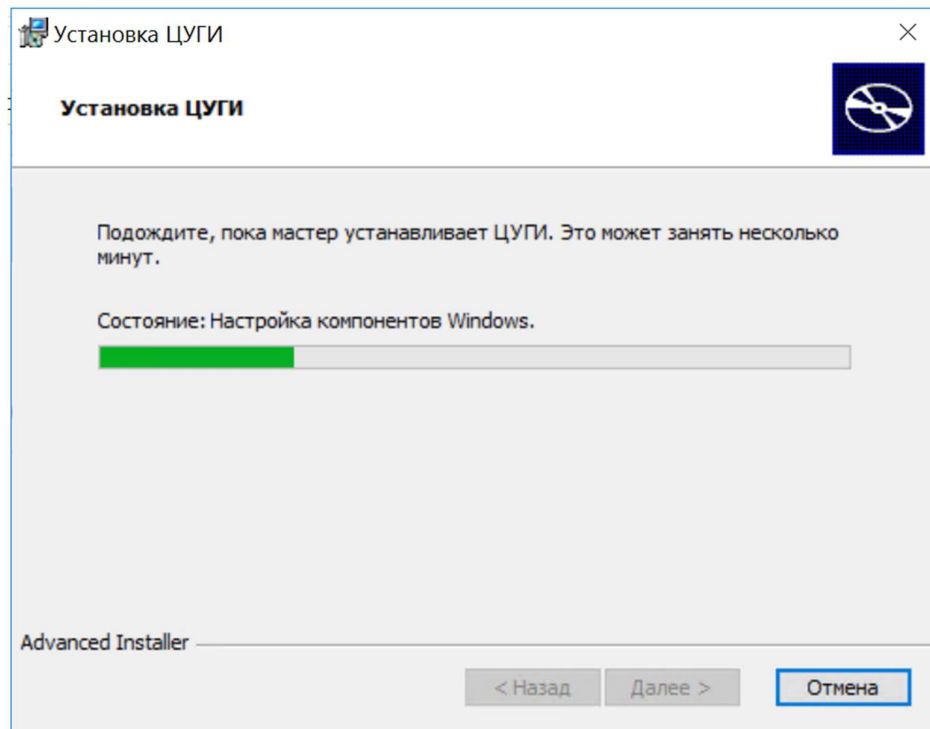


Рисунок 5 – Процесс установки самой системы ЦУГИ.

После распаковки и размещения на диске компонентов системы ЦУГИ, выполняется процесс настройки БД ЦУГИ и системы для работы в односерверной конфигурации.

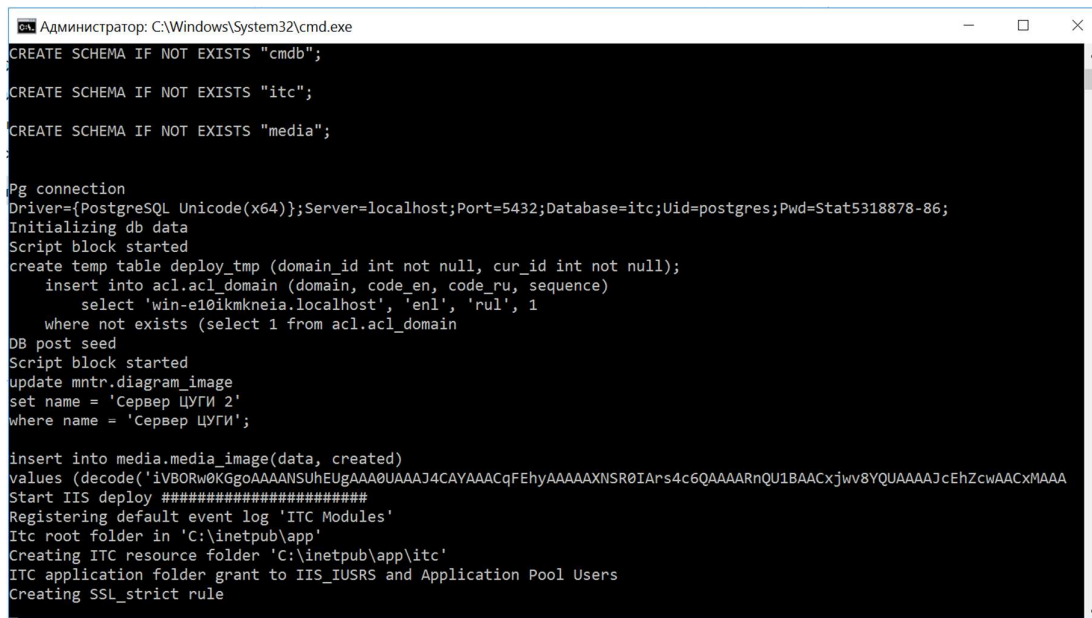


Рисунок 6 – Процесс автоматической настройки системы ЦУГИ.

В процессе установки системы ЦУГИ, открываются окна установки необходимых системных компонентов и сценариев настройки ЦУГИ.

**Важно -** Закрытие промежуточных окон не допускается! При закрытии окон установки и настройки необходимых компонентов ЦУГИ, корректная работа ЦУГИ невозможна!

После завершения установки и настройки компонентов ЦУГИ, выводится окно завершения работы мастера установки ЦУГИ. В окне выводится приглашение для перезагрузки компьютера.

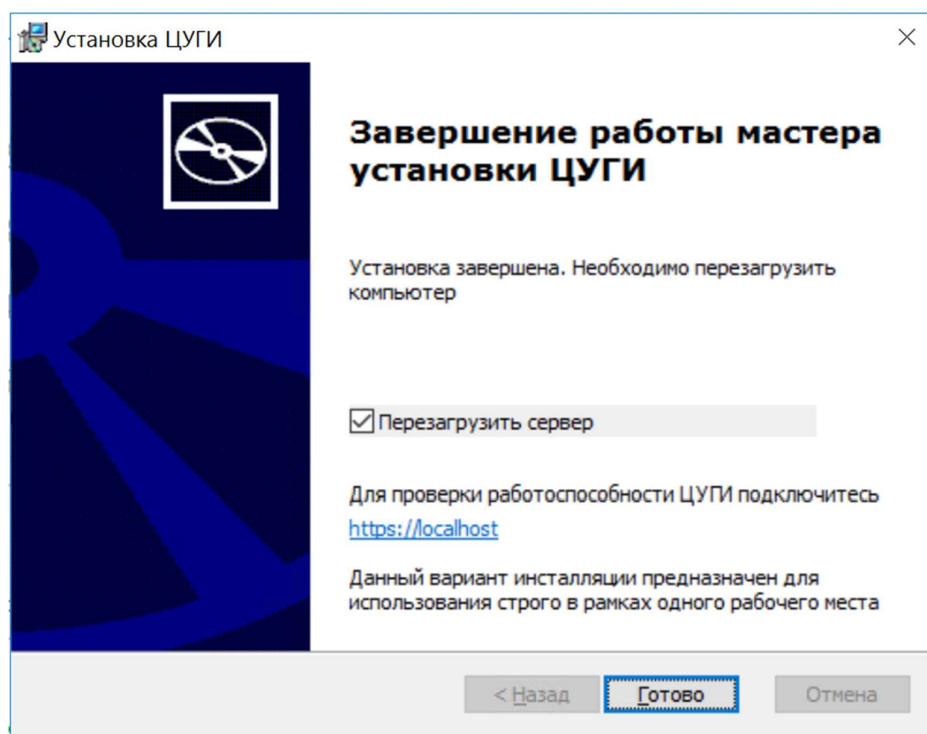


Рисунок 7 – Окно завершения работы мастера установки ЦУГИ и приглашение для перезагрузки сервера.

Перезагрузка сервера необходима для вступления в силу настроек вхождения в группы технических учетных записей, автоматически созданных в процессе установки ЦУГИ. Без перезагрузки сервера после установки, корректная работа ЦУГИ невозможна!

При нажатии на кнопку Готово открывается окно перезагрузки сервера, на который была установлена система ЦУГИ. Необходимо нажать кнопку Да.



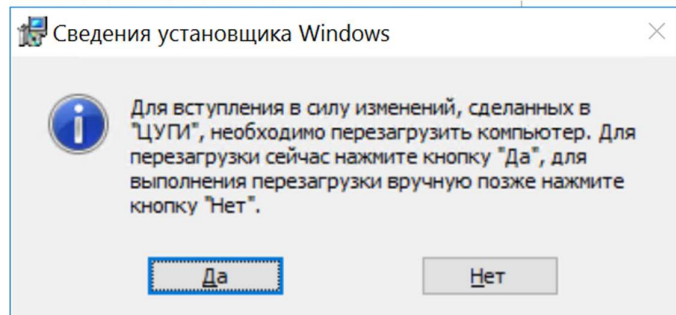


Рисунок 8 – Окно запуска перезагрузки сервера после установки ЦУГИ.

После завершения перезагрузки и входа в операционную систему, система ЦУГИ готова к использованию.

#### 4.7.2 Проверка установки

Для проверки корректности установки ЦУГИ необходимо открыть на сервере поддерживаемую версию браузера и перейти по ссылке <https://localhost>.

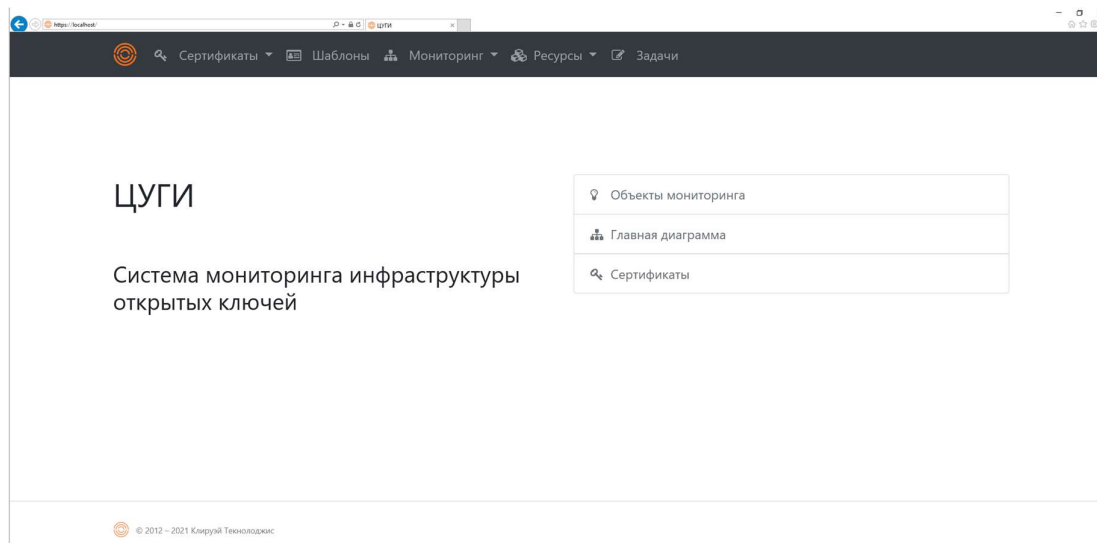


Рисунок 9 – Стартовое окно системы ЦУГИ.

### 4.8 Удаление Сервера ЦУГИ

При корректной установке будет создана запись программы в Панель управления\Все элементы панели управления\Программы и компоненты. Данная запись необходима для возможности удаления серверной части сервиса ЦУГИ. Для удаления программы необходимо выделить мышью в списке установленных программ пункт с именем ЦУГИ и нажать в верхней панели кнопку Удалить, после чего программа будет удалена с жёсткого диска, веб-сервер ЦУГИ удалён из IIS (при удалении программы, используемая база данных на сервере SQL не удаляется).



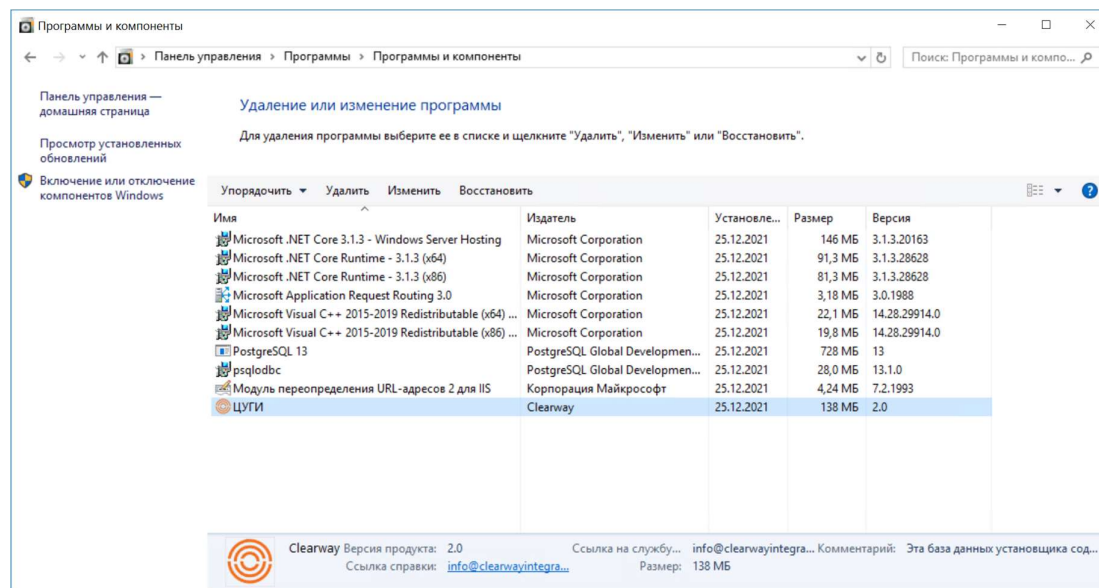


Рисунок 10 – Программа ЦУГИ в списке установленных программ ОС Windows.

## 5 Настройка системы

Далее описаны основные действия по настройке интерфейса и функциональности установленного портала ЦУГИ.

Примечание — Для настройки серверов ЦУГИ рекомендуется обратиться в организацию разработчика.

### 5.1 Настройки ЦУГИ для работы в сетевой конфигурации

Для работы ЦУГИ в сетевой конфигурации необходимо

- определить полное сетевое имя (fully qualified domain name) сервера, на котором установлена система ЦУГИ
- сформировать для сетевого имени закрытый ключ и сертификат SSL, включающий сетевое имя сервера ЦУГИ в поле “Дополнительное имя субъекта”
- импортировать сертификат в хранилище «Личное» для сервера, на котором установлена система ЦУГИ
- настроить компоненты ЦУГИ в диспетчере сервера приложений IIS для использования сертификата SSL
- перезапустить IIS

Для определения полного сетевого имени сервера необходимо открыть окно интерпретатора команд Powershell и вбить команду: `[System.Net.Dns]::GetHostByName($env:computerName).HostName`

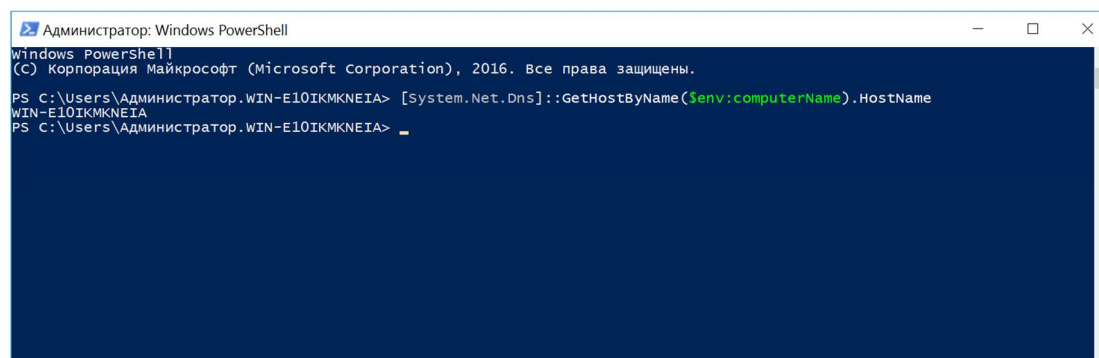


Рисунок 11 – Пример определения полного имени хоста.

Для полученного сетевого имени необходимо сформировать сертификат со свойствами:

Субъект: CN = полное сетевое имя сервера

Дополнительное имя субъекта: DNS = полное сетевое имя сервера

Улучшенный ключ: проверка подлинности клиента, проверка подлинности сервера

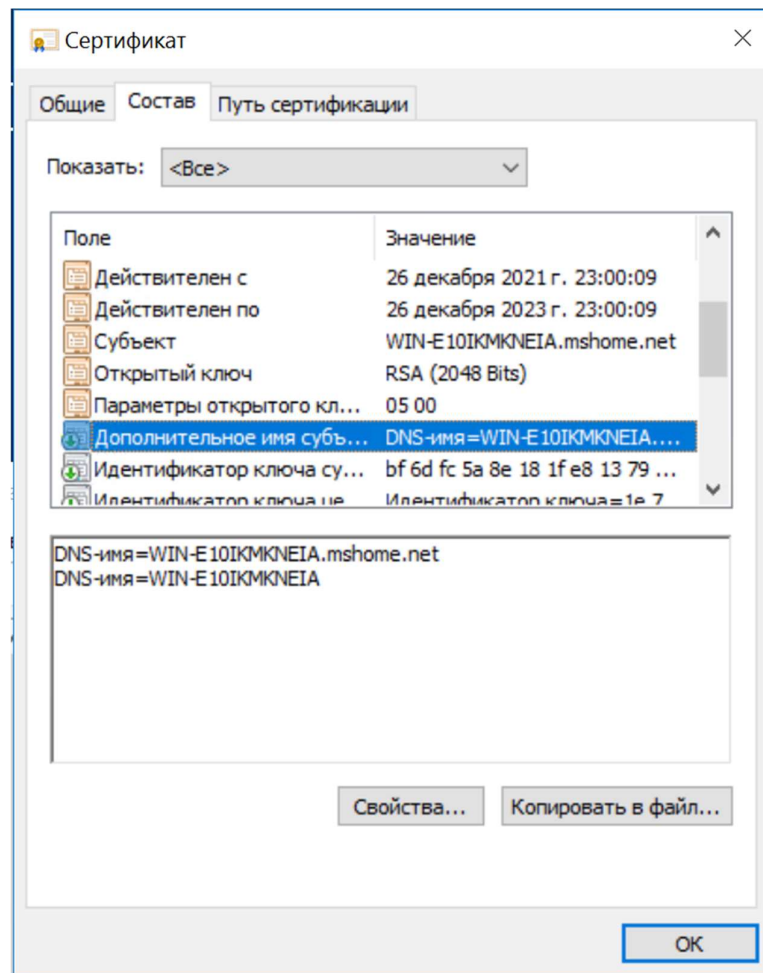


Рисунок 12 – Пример сертификата для сетевой конфигурации сервера ЦУГИ.

Закрытый ключ и такой сертификат можно сгенерировать в ЦС, установленном в сети, где развернута система ЦУГИ, или сгенерировать с помощью общедоступных средств генерации сертификатов, таких как Let's Encrypt.

Полученный сертификат необходимо установить в хранилище сертификатов «Личное» на сервере, где установлена система ЦУГИ. Это позволит указать сертификат в настройках диспетчера сервера приложений IIS, и сделать систему ЦУГИ доступной по безопасному соединению TLS с других компьютеров в сети.

Важно - для импорта сертификата в хранилище «Личное» компьютера пользователь должен обладать правам локального администратора.

Для импорта сертификата необходимо запустить системное приложение «Управление сертификатами компьютеров».

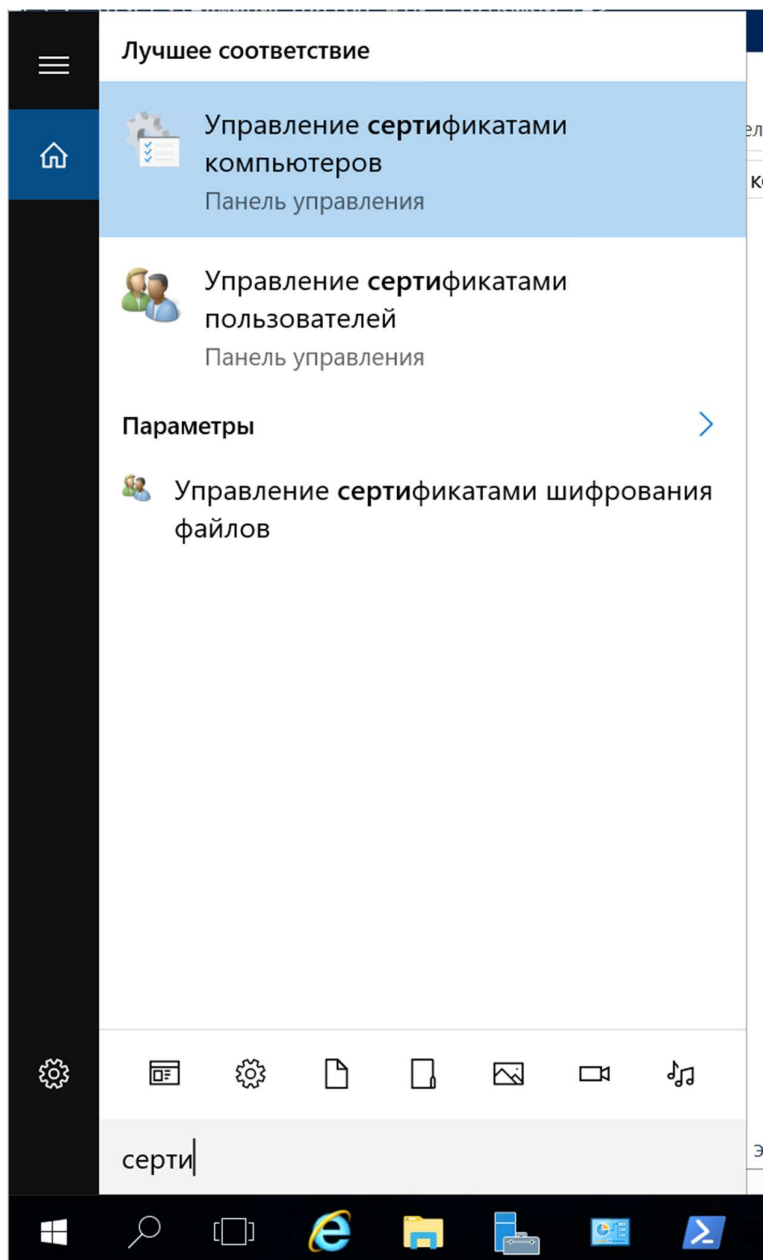


Рисунок 13 – Запуск системного приложения «Управление сертификатами компьютеров»

Далее необходимо открыть хранилище сертификатов «Личное» и в контекстном меню выбрать команду импорта сертификата.

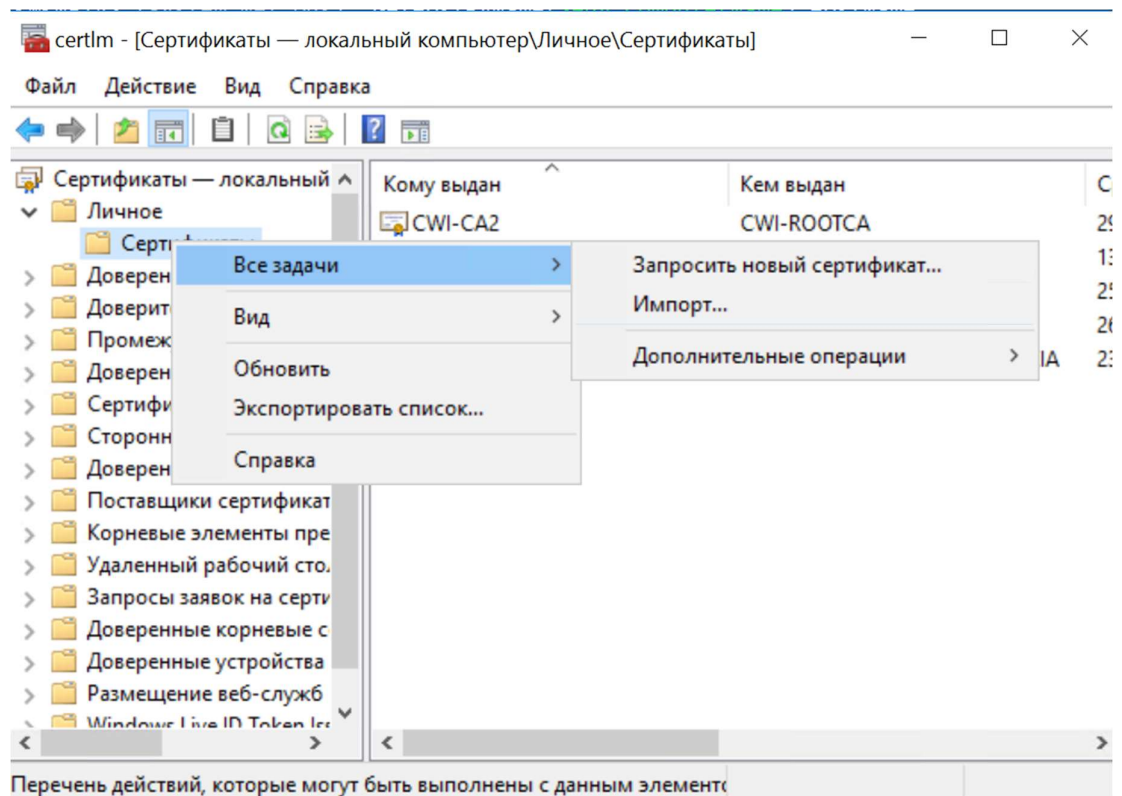


Рисунок 14 – Запуск команды импорта сертификата в контекстном меню хранилища «Личное»

После завершения мастера импорта сертификата, закрытый ключ и сертификат доступны в хранилище «Личное» сертификатов компьютера, на котором установлена система ЦУГИ.

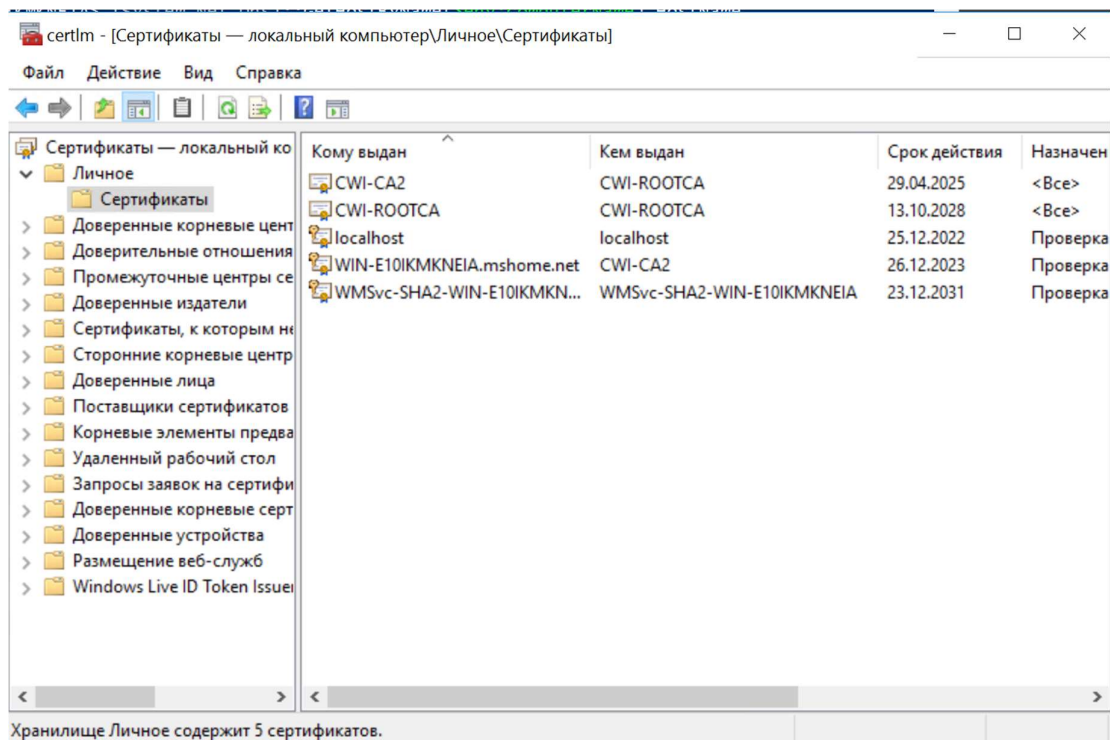


Рисунок 15 – Пример сертификата для сетевого имени сервера ЦУГИ, вместе с автоматически сгенерированным сертификатом localhost для односерверной конфигурации, в хранилище сертификатов сервера

Для настройки компонентов системы ЦУГИ для использования полученного сертификата и привязки компонентов к полному сетевому имени сервера, необходимо запустить системное приложение «Диспетчер служб IIS». Далее в приложении необходимо выбрать сайт Default Web Site и настроить привязку для порта https. Для этого нужно выбрать операцию «Привязки...» в управляющей панели «Действия».

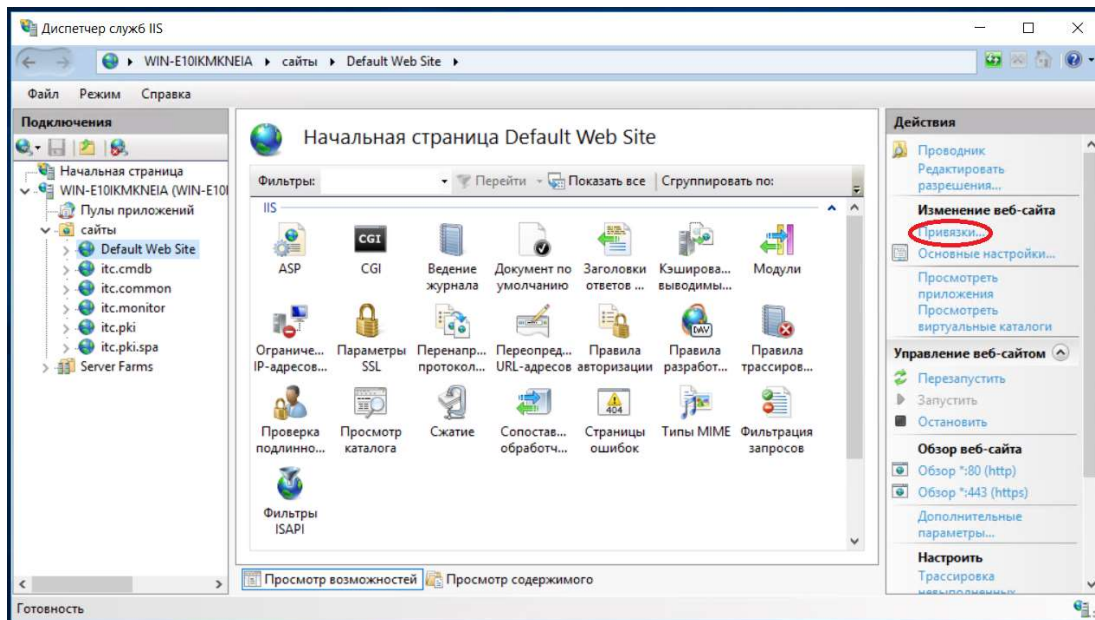


Рисунок 16 – Выбор операции привязки для основного веб-сайта ЦУГИ Default Web Site в приложении Диспетчер служб IIS

Далее необходимо выбрать тип протокола https и нажать кнопку «Изменить».

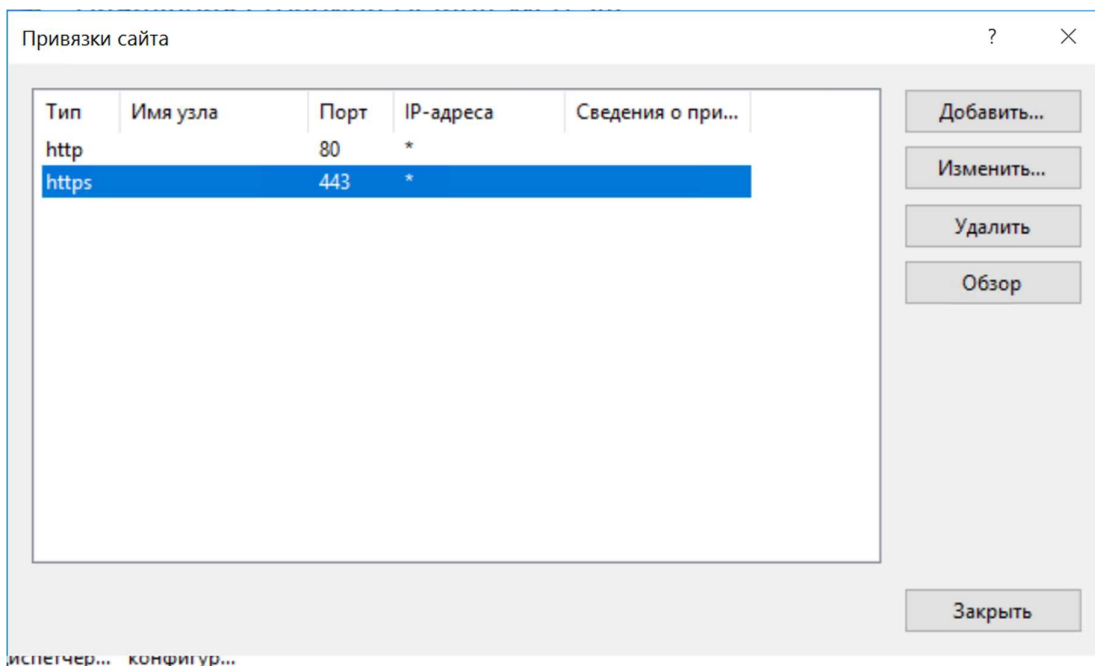


Рисунок 17 – Изменение привязки для протокола https для указания нового сертификата

Далее необходимо выбрать полученный сертификат в селекторе SSL-сертификат и нажать кнопку ОК

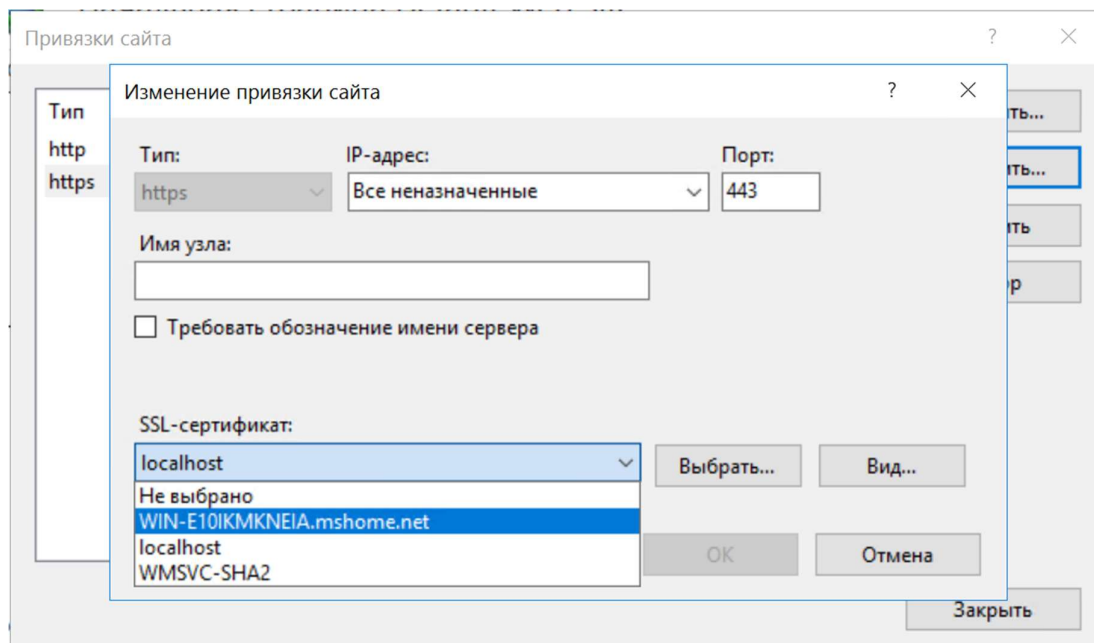


Рисунок 18 – Выбор сертификата с серверным доменным именем в окне изменения привязки для сайта ЦУГИ Default Web Site

Далее необходимо проделать ту же операцию для сайтов – компонентов системы ЦУГИ:

- itc.cmdb
- itc.common
- itc.monitor
- itc.pki
- itc.pki.spa

Для вступления изменений в силу необходимо перезапустить диспетчер сервера приложений IIS. Для этого необходимо выбрать корневой узел (называющийся так же, как сервер) в области «Подключения» в окне приложения Диспетчер служб IIS, и выбрать команду перезапустить в области «Управление сервером»



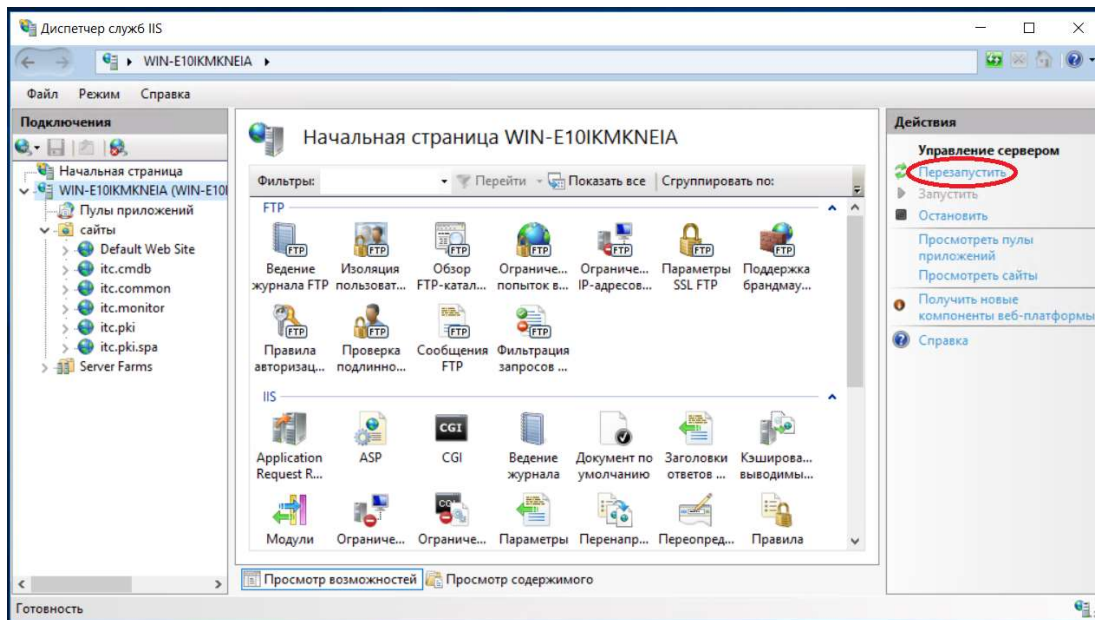


Рисунок 19 – Перезапуск IIS

После этого компоненты системы ЦУГИ, установленные на сервере, доступны по сети по полному сетевому имени сервера, по протоколу https и порту 443. Система ЦУГИ готова к работе в сетевой конфигурации.

## 5.2 Настройка подключения системы ЦУГИ к домену Active Directory

По умолчанию, в односерверной конфигурации система ЦУГИ доступна только пользователю, выполнявшему установку системы. Для подключения к ЦУГИ пользователей из домена Active Directory, необходимо изменить технические учетные записи ЦУГИ на доменные учетные записи, и настроить в конфигурации ЦУГИ путь к серверу Active Directory и корневому домену Active Directory.

Для работы системы ЦУГИ в сетевой конфигурации с подключением к Active Directory в домене Active Directory должны быть созданы следующие технические учетные записи и группы:

| Объект             | Имя            | Назначение                                      | Требуемые права   |
|--------------------|----------------|---|---|
| Учетная запись itc | itc            | Учетная запись для запуска пулов приложений IIS | Сервер ЦУГИ – локальный администратор.  |
| Учетная запись     | Itcintegration | Учетная запись для импорта данных в ЦУГИ        | Сервер ЦУГИ – локальный администратор.<br>Сервер, с которого осуществляется импорт данных в ЦУГИ – локальный администратор. |

|                     |                    |                     |  |
|---------------------|--------------------|---------------------|--|
| Группа безопасности | Itc_administrators | Администраторы ЦУГИ |  |
| Группа безопасности | Itc_users          | Операторы ЦУГИ      |  |

Для обеспечения доступа доменных пользователей ЦУГИ, необходимо перенастроить диспетчер сервера приложений IIS для использования доменной учетной итс для запуска пулов приложений, и настроить подключение ЦУГИ к домену Active Directory для чтения сведений о принадлежности пользователей к группам безопасности ЦУГИ.

Для изменения учетной записи для запуска пулов приложений необходимо запустить системное приложение «Диспетчер служб IIS» и выбрать раздел «Пулы приложений» в области «Подключения».

Далее необходимо выбрать пул itc.pki.pool и команду «Дополнительные параметры...» в области «Изменить пул приложений» панели действий.

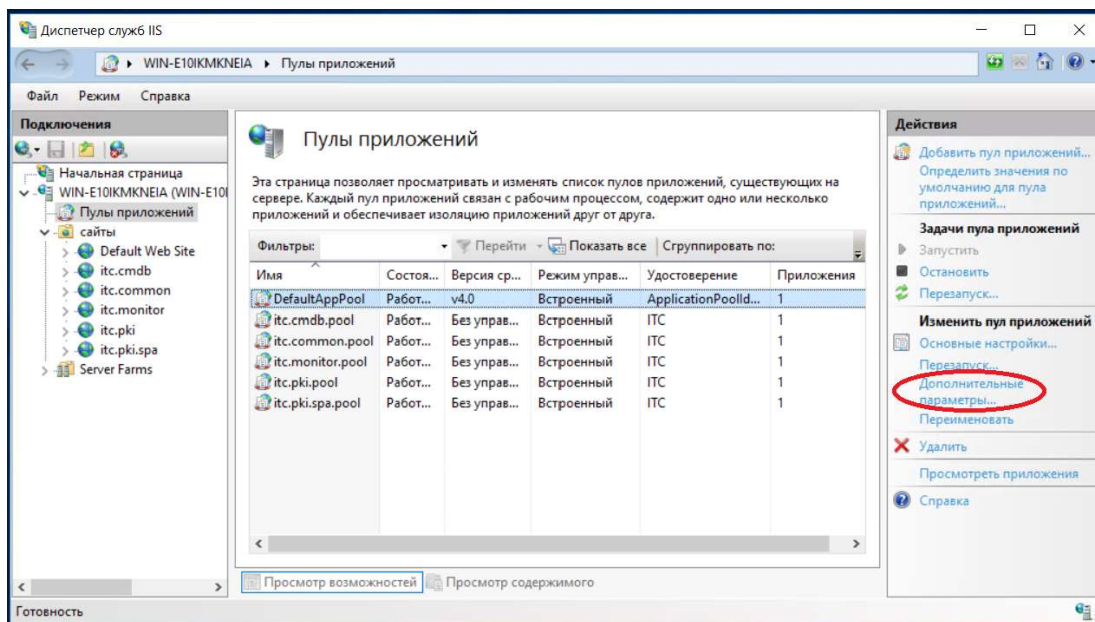


Рисунок 20 – Выбор настройки пулов приложений в диспетчере служб IIS

Далее необходимо выбрать доменную техническую учетную запись itc в опции «Удостоверение» раздела настроек «Модель процесса», и включить опцию «Загружать профиль пользователя».

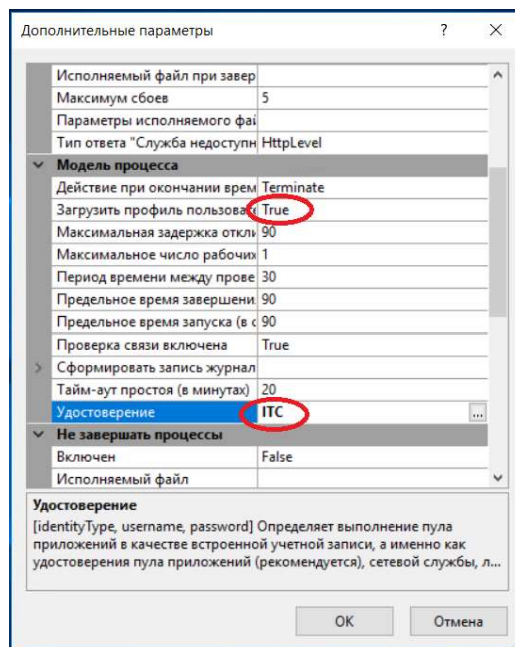


Рисунок 21 – Выбор учетной записи в настройках пула приложений

Для возможности доступа доменной технической учетной записи для интеграции itcintegration необходимо добавить ее в локальную группу itcApiAccess. Для этого нужно запустить системное приложение «Локальные пользователи и группы» (например, нажать клавиши Windows + R и запустить команду lusrmgr.msc). Далее необходимо выбрать раздел «Группы», дважды щелкнуть по группе itcApiAccess, добавить доменную учетную запись itcintegration с помощью кнопку «Добавить» и нажать кнопку ОК.

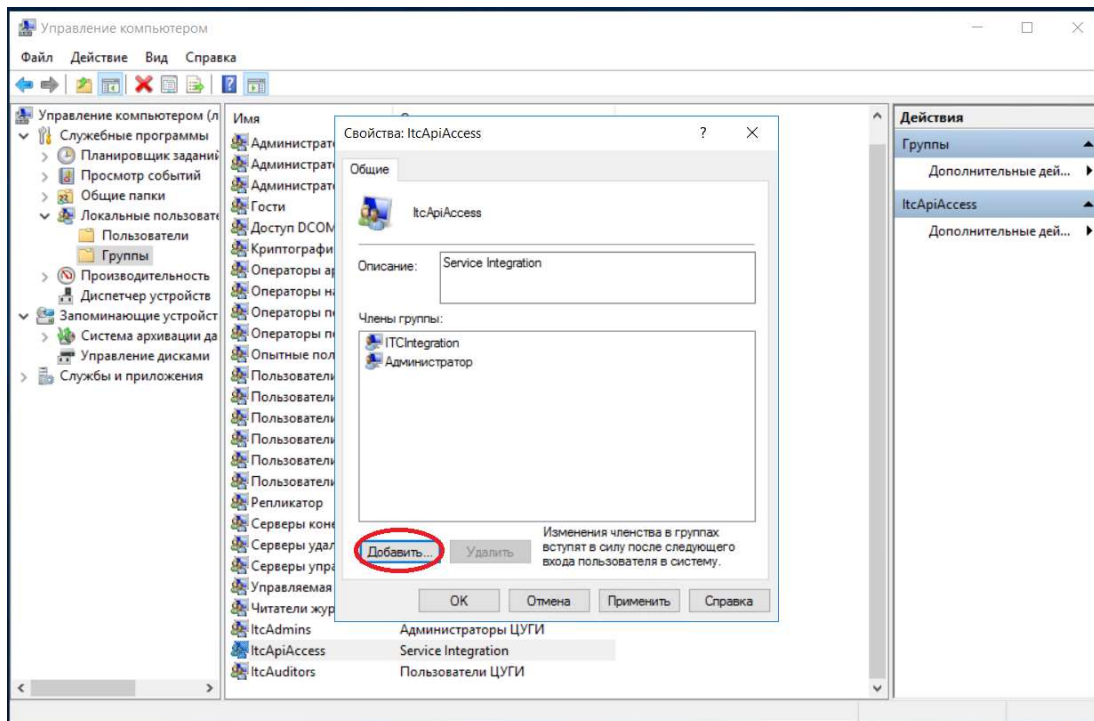


Рисунок 22 – Добавление учетной записи в локальную группу для интеграции

Далее, для подключения к домену Active Directory необходимо открыть файл `c:\inetpub\App\itc\config\itc_config.json`. В разделе `externalServices` в объекте `connection` необходимо в полях `host` и `credential` указать адрес контроллера домена Active Directory. В поле `root` объекта `filters` необходимо указать название корневого OU раздела с пользователями.

После этого необходимо перезапустить диспетчер сервера приложений IIS. Система ЦУГИ в сетевой конфигурации готова для работы с доменными пользователями, и сбора данных с других серверов.

### 5.3 Настройка мониторинга компонентов Сервера

По умолчанию система ЦУГИ настроена в односерверной конфигурации для мониторинга компонентов сервера, на котором установлена система.

Для мониторинга других серверов необходимо в первую очередь настроить систему ЦУГИ для работы в сетевой конфигурации (раздел 5.1) и подключить систему к домену Active Directory (раздел 5.2). Последнее необходимо для того, чтобы скрипты мониторинга, развернутые на других компьютерах в сети, могли безопасно подключиться к компоненту приема данных мониторинга системы ЦУГИ.

Для осуществления мониторинга сервера используются следующие файлы:

- C:\Scripts\itc.get.perfcounters.ps1 – сценарий получения данных;
- C:\Scripts\itc.send.perfcounters.ps1 – сценарий передачи данных на сервер ЦУГИ
- C:\Scripts\New-SchTask.ps1 – сценарий настройки регулярного задания в Планировщике заданий Windows.

Для начала мониторинга необходимо скопировать перечисленные выше файлы в папку C:\Scripts на сервер, мониторинг которого нужно выполнять, с сервера ЦУГИ (файлы копируются автоматически на сервер ЦУГИ при установке).

Далее на целевом сервере, мониторинг которого нужно выполнять, необходимо выполнить с правами локального администратора команду Powershell для регистрации скрипта мониторинга в планировщике задач Windows:

```
C:\scripts\New-SchTask.ps1 -ScriptPath 'C:\scripts\itc.send.perfcounters.ps1 -  
DefaultDomain "mshome.net" -ITCServer "WIN-E10IKMKNEIA.mshome.net"' -TaskName  
"ITC perf monitor task" -User itcintegration@domain
```

где

- значение параметра User это название доменной технической учетной записи itcintegration, включающее название домена
- значение параметра DefaultDomain это название домена
- значение параметра ITCServer это полное сетевое имя сервера ЦУГИ

Скрипт запросит пароль учетной записи, после чего на сервере будет создано задание, раз в 5 минут посылающее данные мониторинга сервера в систему ЦУГИ.

При каждом запуске задачи будет собраны и импортированы на сервер ЦУГИ, следующие данные мониторинга:

- Процессор – статус загрузки центрального процессора. Статус меняется со «Здоров» на «Ошибка» если процессор загружен более чем на 90%;
- Диск – статус системного диска. Статус меняется со «Здоров» на «Ошибка» если место на диске занято более чем на 90%;
- Память – статус загрузки оперативной памяти. Статус меняется со «Здоров» на «Ошибка» если оперативная память используется более чем на 90%;
- Статус сервера – статус объектов для добавления на диаграмму в виде графика.

## 5.4 Настройка мониторинга компонентов ИОК

Подключение системы ЦУГИ в сетевой конфигурации к ЦС и настройка мониторинга компонентов ИОК выполняется специалистами организации разработчика.

## 5.5 Настройка диаграмм

Для добавления или удаления диаграммы нужно зайти в меню «Диаграммы» и выбрать пункт «Список диаграмм».

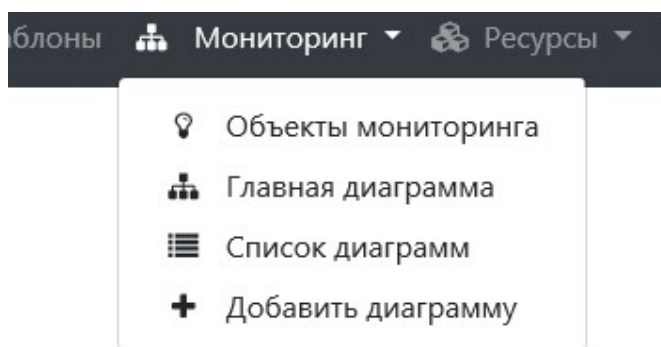


Рисунок 23 — Меню «Диаграммы».

В списке диаграмм можно выполнить следующие действия:

удалить существующую диаграмму — для этого нужно нажать значок корзины напротив соответствующей диаграммы;

сделать диаграмму основной — для этого нужно нажать на кнопку со значком стрелки напротив выбранной диаграммы;

добавить новую диаграмму — для этого нужно нажать кнопку «+ Добавить диаграмму».

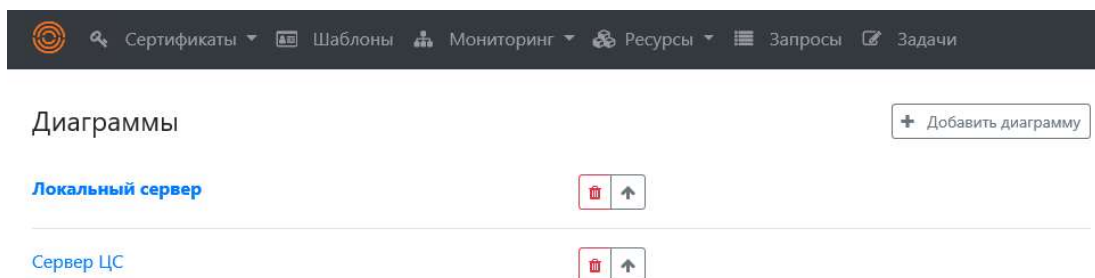


Рисунок 24 — Интерфейс для настройки диаграмм.

В случае добавления новой диаграммы появится диалоговое окно, в котором можно выбрать графический файл и указать имя диаграммы. После этого нужно нажать кнопку «Сохранить».

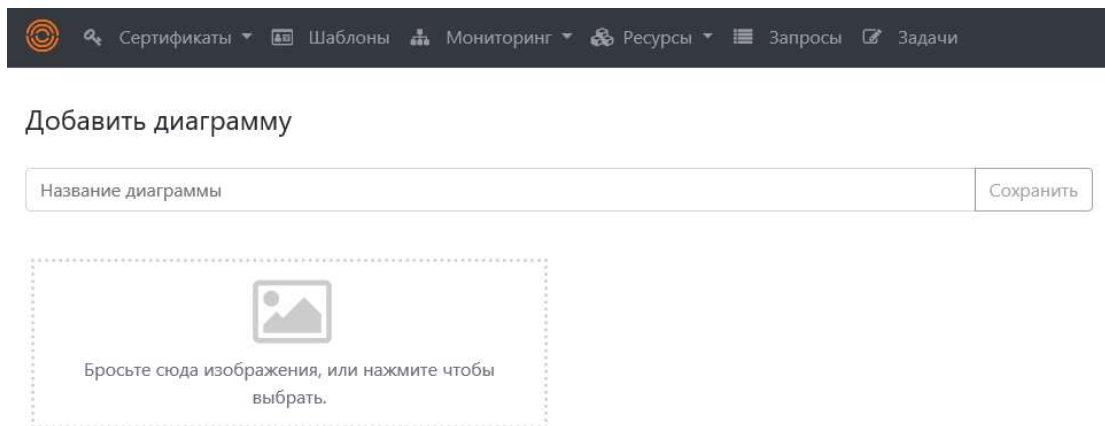


Рисунок 25 — Интерфейс для добавления диаграммы.

После добавления подложки на диаграмму нужно нанести объекты. Они могут быть следующих типов:

- объект мониторинга;
- ссылка;
- диаграмма (график).

Для их добавления нужно нажать синюю кнопку в правом нижнем углу (см. рисунок ниже).

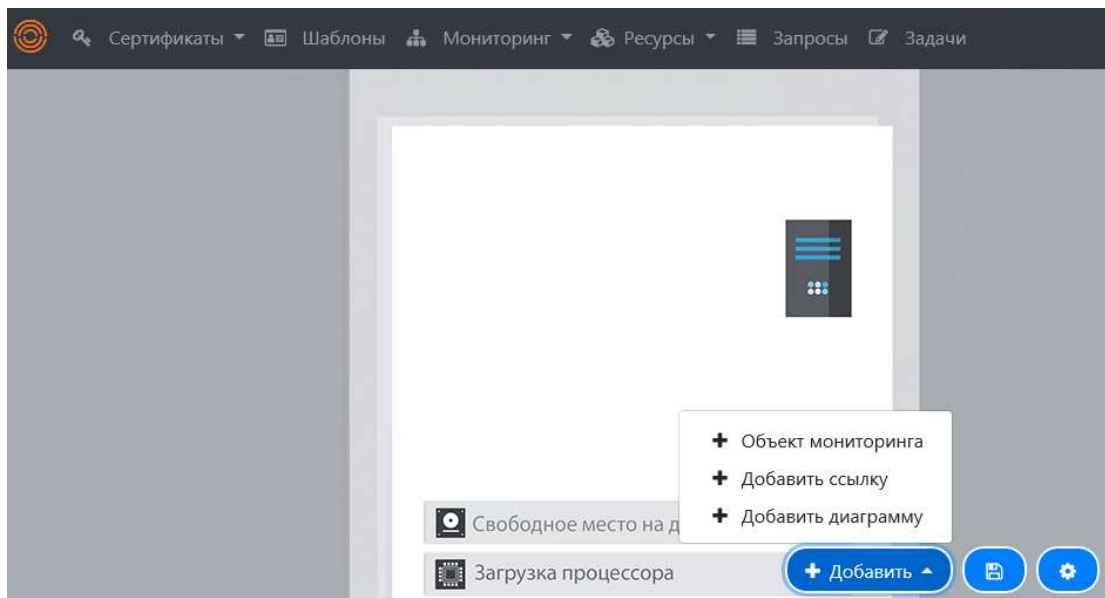


Рисунок 26 — Интерфейс для добавления объектов на подложку.



После этого откроется страница со списком объектов. Для добавления объекта нужно отметить его и нажать кнопку «Выбрать» (см рисунок ниже).

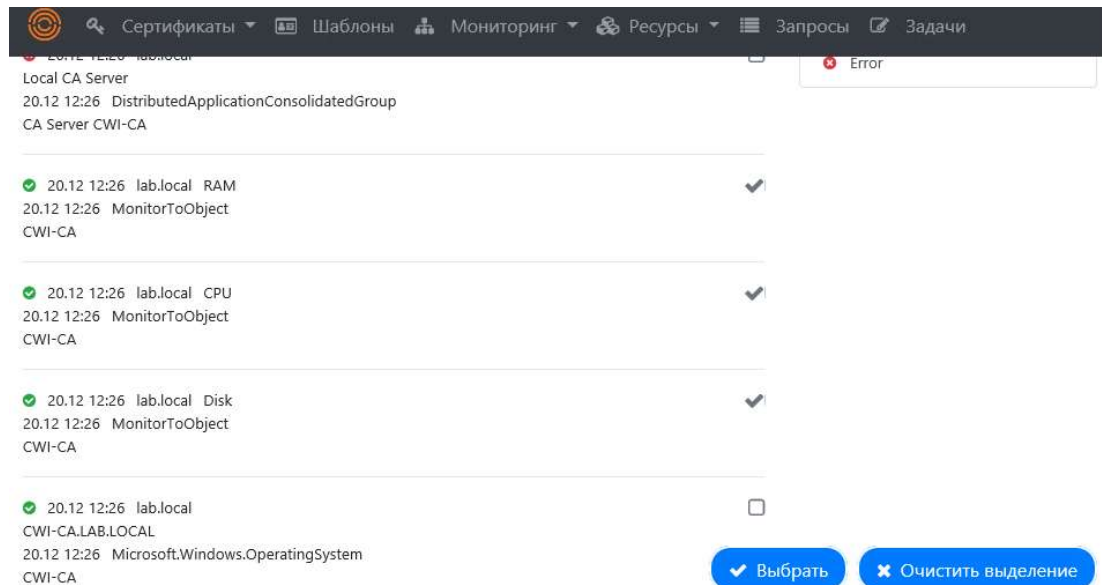


Рисунок 27 — Интерфейс для выбора и добавления объектов мониторинга.

После добавления объекта его можно перемещать по подложке. Также возможно добавление ссылки на объект. При нажатии на объект со ссылкой произойдёт переход на указанный в ссылке компонент интерфейса. Объекты мониторинга могут отображаться в виде значка или области.

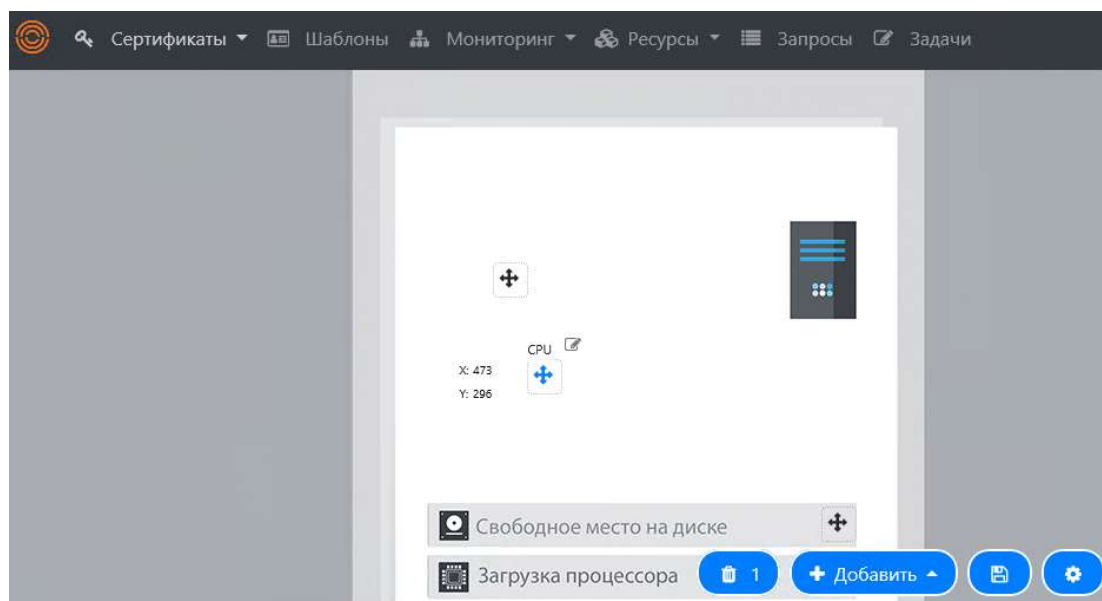




Рисунок 28 — Перемещение объектов мониторинга по подложке

## 5.6 Настройка функции «Сертификаты с ЦС»

Система ЦУГИ позволяет импортировать сертификаты с ЦС различных производителей для дальнейшей обработки и мониторинга.

Подключение системы ЦУГИ в сетевой конфигурации к ЦС и настройка импорта сертификатов ЦС выполняется специалистами организации разработчика.

## 5.7 Настройка «Сертификаты с серверов»

Система ЦУГИ позволяет импортировать сертификаты из локального хранилища сертификатов сервера(ов) для дальнейшей обработки и мониторинга.

По умолчанию, в односерверной конфигурации система ЦУГИ при установке автоматически разово загружает сертификаты с сервера, на который устанавливается система.

Для чтения сертификатов других серверов необходимо в первую очередь настроить систему ЦУГИ для работы в сетевой конфигурации (раздел 5.1) и подключить систему к домену Active Directory (раздел 5.2). Последнее необходимо для того, чтобы скрипты импорта сертификатов, развернутые на других компьютерах в сети, могли безопасно подключиться к компоненту приема данных мониторинга системы ЦУГИ.

Для осуществления импорта сертификатов используются следующие файлы:

- C:\Scripts\itc.read.computer.certs.ps1 – сценарий получения данных;
- C:\Scripts\itc.send.computer.certs.ps1 – сценарий передачи данных на сервер ЦУГИ;
- C:\Scripts\New-SchTask.ps1 – сценарий настройки регулярного задания в Планировщике заданий Windows.

Для регулярного импорта сертификатов с сервера необходимо скопировать перечисленные выше файлы в папку C:\Scripts на сервер, сертификаты которого нужно импортировать, с сервера ЦУГИ (файлы копируются автоматически на сервер ЦУГИ при установке).

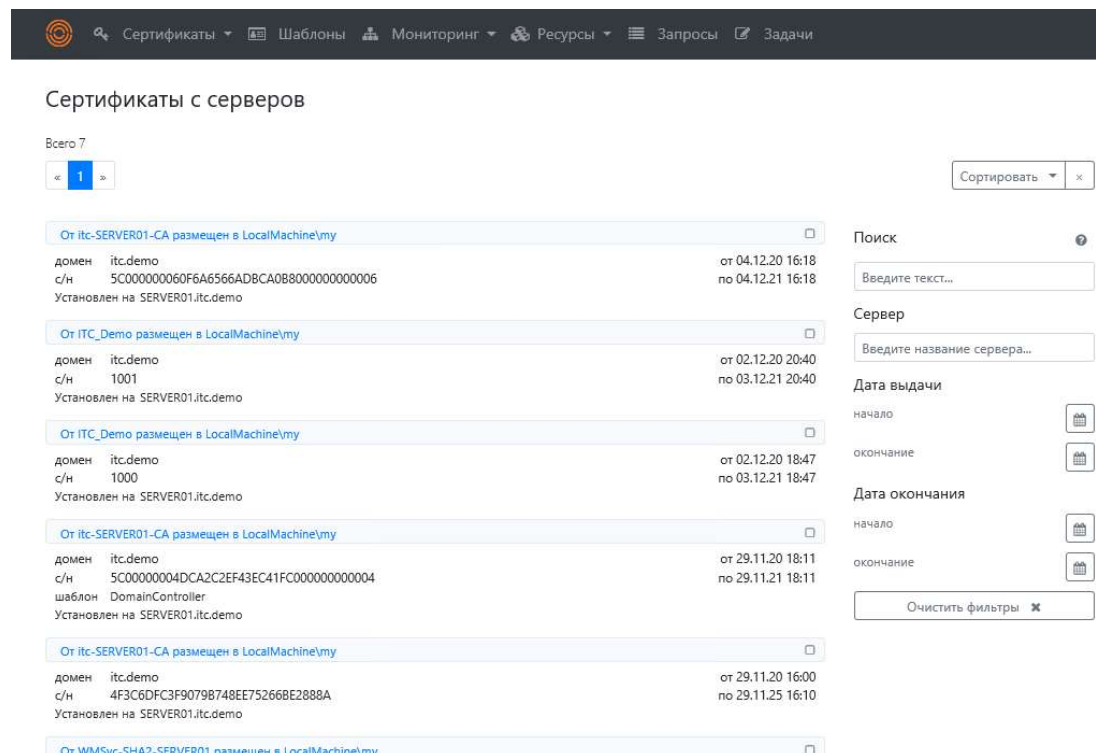
Далее на целевом сервере, сертификаты которого, необходимо выполнить с правами локального администратора команду Powershell для регистрации скрипта мониторинга в планировщике задач Windows:

```
C:\scripts\New-SchTask.ps1 -ScriptPath 'C:\scripts\itc.send.computer.certs.ps1 -DefaultDomain "mshome.net" -ITCServer "WIN-E10IKMKNEIA.mshome.net"' -TaskName "ITC certs import task" -RepetitionPeriodMinutes 1440 -User itcintegration@domain
```

где

- значение параметра User это название доменной технической учетной записи itcintegration, включающее название домена
- значение параметра DefaultDomain это название домена
- значение параметра ITCServer это полное сетевое имя сервера ЦУГИ
- значение параметра RepetitionPeriodMinutes это частота повторения импорта сертификатов в минутах

Скрипт запросит пароль учетной записи, после чего на сервере будет создано задание, раз в 24 часа читающее сертификаты сервера из хранилища “Личное” и отправляющее сертификаты в систему ЦУГИ.



Сертификаты с серверов

Всего 7

Сортировать

| Источник  | Домен    | С/н                                    | Установлен на     | От             | По             |
|---|----------|--|-------------------|----------------|----------------|
| От itc-SERVER01-CA размещен в LocalMachine\my     | itc.demo | 5C000000060F6A6566ADBCA0880000000000   | SERVER01.itc.demo | 04.12.20 16:18 | 04.12.21 16:18 |
| От ITC_Demo размещен в LocalMachine\my            | itc.demo | 1001                                   | SERVER01.itc.demo | 02.12.20 20:40 | 03.12.21 20:40 |
| От ITC_Demo размещен в LocalMachine\my            | itc.demo | 1000                                   | SERVER01.itc.demo | 02.12.20 18:47 | 03.12.21 18:47 |
| От itc-SERVER01-CA размещен в LocalMachine\my     | itc.demo | 5C00000004DCA2C2EF43EC41FC000000000004 | DomainController  | 29.11.20 18:11 | 29.11.21 18:11 |
| От itc-SERVER01-CA размещен в LocalMachine\my     | itc.demo | 4F3C6DFC3F90798748EE752668E2888A       | SERVER01.itc.demo | 29.11.20 16:00 | 29.11.25 16:10 |
| От WMSvc-SHA2-SERVER01 размещен в LocalMachine\my |          |  |                   |                |                |

Поиск: Введите текст...

Сервер: Введите название сервера...

Дата выдачи: начало, окончание

Дата окончания: начало, окончание

Очистить фильтры

Рисунок 29 — Сертификаты с серверов

### 5.7.1 Оповещения об истекающих сертификатах с серверов

Подключение системы ЦУГИ в сетевой конфигурации к почтовому серверу, настройка частоты формирования оповещений, списка получателей и критериев отбора сертификатов, по которым должны формироваться оповещения об истечении срока действия, выполняется специалистами организации разработчика.

## 5.8 Настройка «Шаблоны»

Система ЦУГИ позволяет импортировать шаблоны сертификатов, опубликованные в ЦС, для дальнейшей обработки и мониторинга.

Подключение системы ЦУГИ в сетевой конфигурации к ЦС и настройка импорта шаблонов сертификатов ЦС выполняется специалистами организации разработчика.

## 5.9 Настройка функции «Сводная таблица»

Сводная таблица предназначена для наглядной демонстрации статусов мониторинга нескольких серверов и ЦС на одной веб странице.

Для добавления статуса мониторинга объекта на сводную таблицу, данный объект нужно выбрать в списке «Объекты мониторинга» и нажать «+Добавить в сводную таблицу».

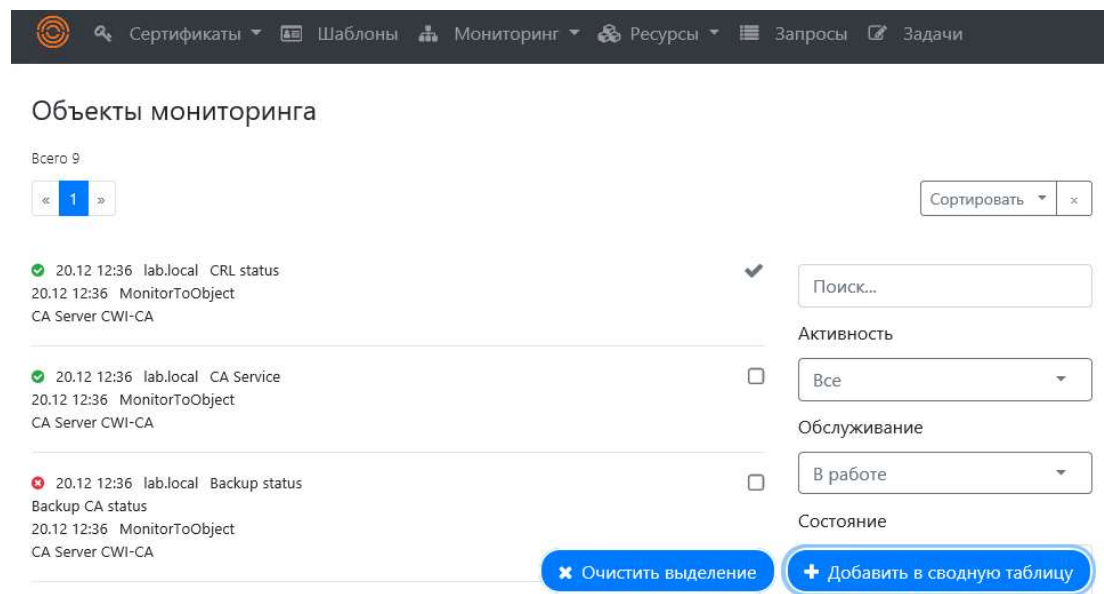
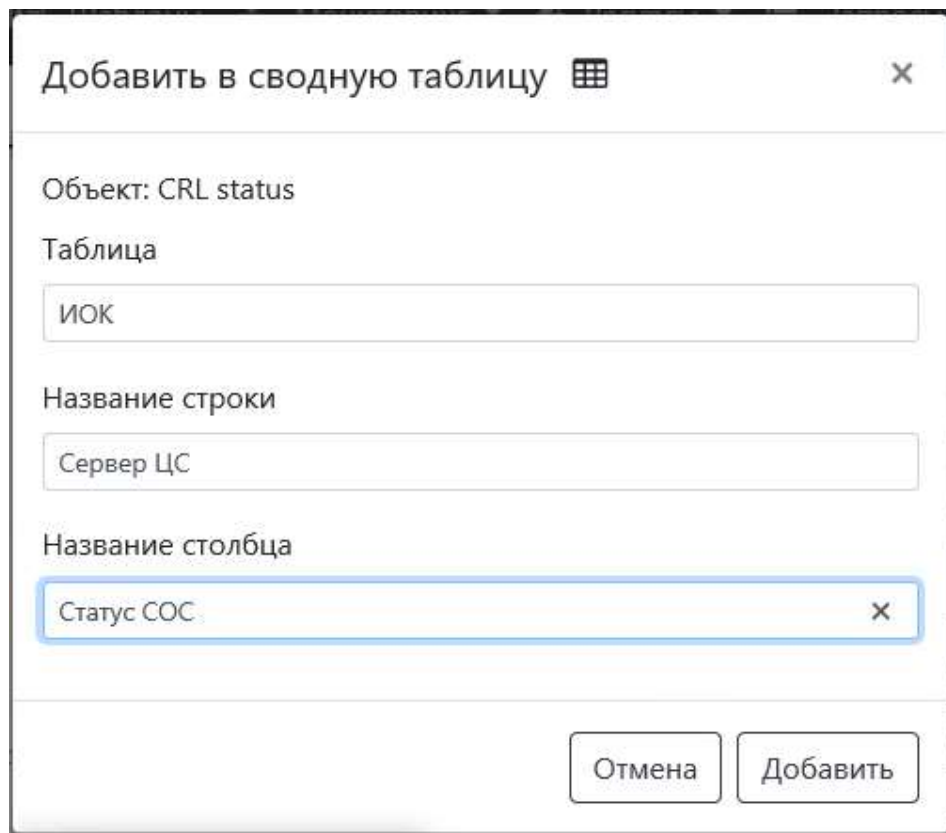



Рисунок 30 — Добавление объекта на сводную таблицу.

Далее появится окно указать имя таблицы (если создается впервые) строк и столбцов для добавления в таблицу (строки можно указывать новые или выбирать из созданных ранее).



Добавить в сводную таблицу 

Объект: CRL status

Таблица

ИОК

Название строки

Сервер ЦС

Название столбца

Статус СОС

Отмена Добавить

Рисунок 31 — Указание строки и столбца в сводной таблице для добавляемого объекта.

## 5.10 Настройка функции «ИОК резервное копирование»

Система ЦУГИ может осуществлять регулярное резервное копирование настроек ЦС.

Подключение системы ЦУГИ в сетевой конфигурации к ЦС и настройка заданий регулярного резервного копирования ЦС выполняется специалистами организации разработчика.

## 5.11 Настройка функции «Запросы» сертификатов

Система ЦУГИ в сетевой конфигурации при условии подключения к ЦС поддерживает функционал формирования запроса и выдачи сертификата с ЦС.

Подключение системы ЦУГИ в сетевой конфигурации к ЦС и выполняется специалистами организации разработчика.

## 5.12 Предоставление доступа

Доступ пользователей к функциям и операциям в ЦУГИ определяется принадлежностью пользователя к одной или нескольким Ролям. В базовой поставке ЦУГИ содержит Роли только по умолчанию, которые предполагают следующую модель функционирования:

- Оператор – Сотрудник службы поддержки ИТ, который назначен выполнять процедуры мониторинга состояния ИТ систем. Оператор непрерывно выполняет операции мониторинга с использованием ЦУГИ, участвует в решении задач в части предоставления и интерпретации данных мониторинга, составлении отчётов по данным мониторинга. Выполняет типовые операции по настройке конфигурационных единиц, которые определены в решениях задач.
- Администратор – Сотрудник службы ИТ, осуществляющий настройку работы портала ЦУГИ и имеющий права на управление группами и учётными записями пользователей в службе каталогов.

Ролевой модели соответствуют следующие группы доступа, которые создаются в процессе установки ЦУГИ:

- Администратор - ITC\_Administrators;
- Оператор - ITC\_Users.

Функциональность портала ЦУГИ предусматривает создание новых Ролей и назначение им прав доступа к функциям портала, а также изменение Ролей, созданных по умолчанию.

Предоставление доступа к ЦУГИ осуществляется путем добавления учетной записи пользователя в соответствующую группу.

## 6 Аварийные ситуации

Аварийные ситуации при эксплуатации системы могут возникать в следующих случаях:

- выхода из строя компонентов портала ЦУГИ;
- выхода из строя смежных систем, от которых зависит работоспособность портала ЦУГИ.

Работоспособность ЦУГИ зависит от следующих систем:

- Служба каталога Active Directory;
- Информационная сеть организации Заказчика;

В случае неработоспособности портала ЦУГИ по причине выхода из строя смежной системы администратор оповещает ответственных за соответствующую систему в порядке, установленном регламентами организации Заказчика.

В случае неработоспособности непосредственно ЦУГИ администратор предпринимает действия по быстрому восстановлению работоспособности Системы в соответствии с его квалификацией и опытом работы.

Для решения вопросов связанных с устранением аварийных ситуаций или эксплуатацией ЦУГИ администратор может обратиться в службу поддержки разработчика по адресу электронной почты [support@clearwayintegration.com](mailto:support@clearwayintegration.com).  
Режим работы службы поддержки: с 9:00 до 17:00 по рабочим дням.

### 6.1 Резервное копирование ЦУГИ

Для организации резервного копирования ЦУГИ, необходимо регулярно создавать резервные копии следующих компонентов:

- файлы конфигурации ЦУГИ – файлы, расположенные (по умолчанию) в папке C:\inetpub\App\itc;
- файлы мониторинга и импорта данных – файлы, расположенные (по умолчанию) в папке C:\Scripts;
- база данных ЦУГИ – база данных ЦУГИ.

Так же возможно осуществлять резервное копирование целиком виртуальной машины, на которой развернуты компоненты ЦУГИ.

### 6.2 Восстановление системы из резервной копии ЦУГИ

В случае выхода одно или нескольких компонентов ЦУГИ они восстанавливаются из резервной копии.

Файлы конфигурации, мониторинга и импорта данных восстанавливаются методом их замены на файлы из резервной копии.

База данных восстанавливается из резервной копии штатными средствами СУБД.

В случае если восстановление одного или нескольких компонентов ЦУГИ не привело к ожидаемому результату, рекомендуется установить ЦУГИ заново, далее заменить файлы конфигурации, мониторинга и импорта данных файлами из резервной копии, а базу данных созданную при новой установке заменить на БД из резервной копии.

В случае, когда резервное копирование осуществляется методом создания копии ВМ ЦУГИ, то система восстанавливается целиком как виртуальная машина.