Настройка параметров системы

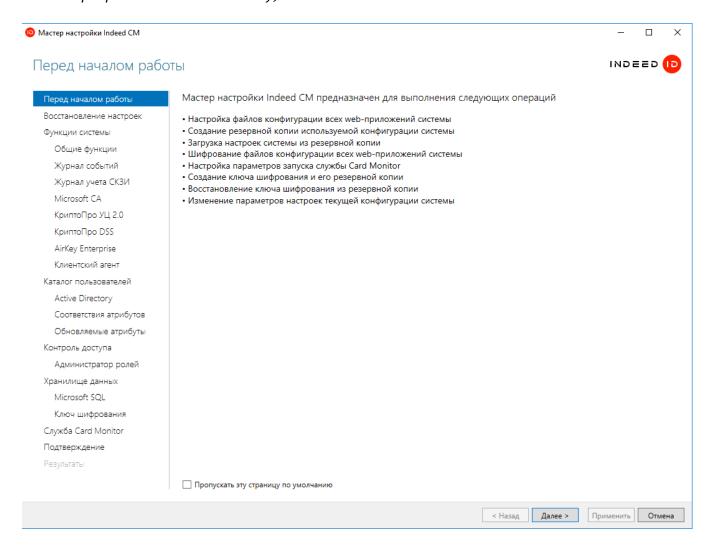
На этапе развертывания системы необходимо указать нужные значения в файлах конфигурации для каждого сервиса. Файлы конфигурации всех сервисов системы располагаются в корневом каталоге веб-приложений IIS (путь по умолчанию % SystemDrive%\inetpub\wwwroot).



Файлы конфигурации сервиса Card Monitor расположены в **%ProgramFiles%\Indeed CM\CardMonitor**.

Настройка файлов конфигурации осуществляется при помощи **Мастера настройки Indeed СМ**. Мастер настройки запускается автоматически после завершения работы Мастера установки сервера Indeed СМ, если в последнем отмечена соответствующая опция.

Также Macтep настройки Indeed CM может быть запущен в любой момент вручную (*Пуск* – *Bce программы – Indeed Identity*).



В Таблице 5 приведены разделы Мастера установки с описанием параметров, которые могут быть в них определены.

Таблица 5 – Разделы мастера настройки Indeed CM и их описание.

Раздел	Описание
Перед началом работы	Информация о назначении и возможностях мастера настройки Indeed CM.
Восстановление настроек	Загрузка файла резервной копии конфигурации Indeed CM.
Функции системы:	Общие функции: настройка внутренних параметров web-приложений Indeed CM.
 Общие функции Журнал событий Журнал учета СКЗИ Місгоsoft СА КриптоПро УЦ 2.0 КриптоПро DSS АігКеу Ептегргізе Клиентский агент 	 Интеграция с Indeed Access Manager Интеграция с Secret Net Studio Просмотр содержимого устройства в сервисе самообслуживания Просмотр SO PIN устройства Собственная организационная структура Сброс пароля пользователя в Active Directory Включить журнал учета Журнал учета реализован только для конфигурации системы с использованием Хранилища данных в MS SQL.
	 Журнал событий: Переопределять атрибут имени пользователя для поиска в Журнале событий. Значение по умолчанию: CN(common name) Настройка подключения к единому журналу событий для нескольких серверов Indeed CM Журнал учета СКЗИ: настройка параметров ведения журнала учета СКЗИ. Удостоверяющие центры: настройка параметров работы с центрами сертификации. КриптоПро DSS: настройка интеграции с ПАК КриптоПро DSS. AirKey Enterprise: настройка интеграции с сервером виртуальных смарт-карт Indeed AirKey Enterprise. Клиентский агент: настройка параметров работы клиентского агента Indeed CM.
Каталог пользователей: • Active Directory • КриптоПро УЦ 2.0 • Active Directory + КриптоПро УЦ 2.0	Определение каталога пользователей системы. Параметры подключения отображаются в зависимости от выбранного каталога.

Соответствия атрибутов

Определение атрибутов, с которыми необходимо создать нового пользователя в Центре Регистрации КриптоПро УЦ 2.0 с использованием Indeed CM в момент выпуска устройства.

Например: создать нового пользователя в ЦР КриптоПро с теми значениями атрибутов, которые есть для существующего пользователя Active Directory.

Обновляемые атрибуты

Определение списка атрибутов пользователя при изменении которых необходимо обновление сертификата.

В список отслеживаемых атрибутов пользователя в параметрах шаблонов сертификатов Microsoft CA и КриптоПро УЦ 2.0 по умолчанию включены:

- Общее имя(CN)
- E-mail
- UPN-имя пользователя



 Отслеживание изменений в атрибутах пользователей доступно для атрибутов указанных в полях **Субъект** (Subject) и **Дополнительное имя субъекта** (Subject Alternative Name) сертификата.

Контроль доступа:

Определение параметров доступа к сервисам Indeed CM.

• Администратор ролей

Определение учетной записи для первоначальной настройки привилегий пользователей в разделе Роли Консоли управления Indeed Certificate Manager.



Указанная учетная запись должна входить в каталог пользователей системы.

Хранилище данных:

- Active Directory или Microsoft SQL
- Ключ шифрования

Определение хранилища данных системы, алгоритма шифрования данных. Создание резервной копии ключа шифрования и восстановление ключа из копии. Параметры подключения к хранилищу определяются в зависимости от выбранного типа.

Служба Card Monitor

Служба Card Monitor предназначена для выполнения операций по контролю за обращением смарт-карт и выполняет:

- Отзыв карт удаленных пользователей
- Отзыв временных карт с истекшим сроком действия
- Выключение (опционально) карт пользователей, чьи учетные записи Active Directory были отключены
- Установку и сброс статуса содержимого устройства (истекает/истекло)
- Обновление содержимого устройств

🕕 Если обновление устройства проводилось через Агент Indeed СМ без автоматического одобрения сертификатов оператором УЦ.

- Рассылку почтовых уведомлений администраторам и пользователям системы:
 - Истечение срока действия сертификатов пользователей, хранящихся на карте
 - Одобрение/отклонение выпуска карты
 - Одобрение/отклонение обновления сертификатов на карте
 - Одобрение/отклонение замены карты
 - Изменение политики, действующей на пользователя

🕕 Для выполнения задач по регулярному запуску службы Card Monitor, учетная запись, указываемая в мастере настройки должна состоять в группе **Администраторов** (Administrators) на сервере Indeed СМ и иметь разрешение на **Вход в качестве пакетного задания** (Log on as a batch job).

Если для данной учетной записи изменился пароль, то для работы Card Monitor необходимо в Мастере настройки Indeed СМ передобавит ь пользователя, указав новое значение пароля.

Подтверждение

Сводная информация по настройкам всех разделов Мастера с возможностью создания резервной копии конфигурации Indeed CM.

Результаты

Прогресс работы Мастера по записи указанных значений в файлы конфигурации сервисов Indeed CM.

Для работы Card Monitor в разделе **Конфигурация > Роли** потребуются создать сервисную роль, включить в нее учетную запись, от имени которой будет работать Card Monitor и определить для роли привилегии:

- Выключение устройства
- Обновление устройства
- Отзыв устройства
- Отвязка устройства
- Очистка устройства
- Удаление устройства

- Выключение устройства КриптоПро DSS
- Обновление устройства КриптоПро DSS

- Отзыв устройства КриптоПро DSS
- Удаление устройства КриптоПро DSS
- Удаление AirKey



🔼 Если настроена интеграция с КриптоПро DSS и AirKey Enterprise, то задайте привилегии для работы с данными устройствами.

При первой установке Indeed CM настройте необходимые параметры и сохраните их копию (опция Сохранить резервную копию параметров конфигурации в разделе Подтверждение).

Резервная копия настроек Indeed CM включает в себя все параметры, определенные при установке системы для всех сервисов, а также алгоритм и ключ шифрования данных. При развертывании новых серверов Indeed CM используйте файл резервной копии, указав его в разделе Восстановление настроек Мастера установки и настройки.

 Файл резервной копии содержит данные сервисных учетных записей (для работы с каталогом пользователей и хранилищем данных), алгоритм и ключ шифрования. Храните файл резервной копии в защищенном месте.

После завершения работы Мастера настройки Indeed CM указанные значения для всех параметров будут записаны в файлы конфигурации всех приложений и зашифрованы. Шифрование осуществляется при помощи машинного ключа шифрования Microsoft .NET (NetFrameworkConfigurationKey). Алгоритм шифрования – RSA.