

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).

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

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

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

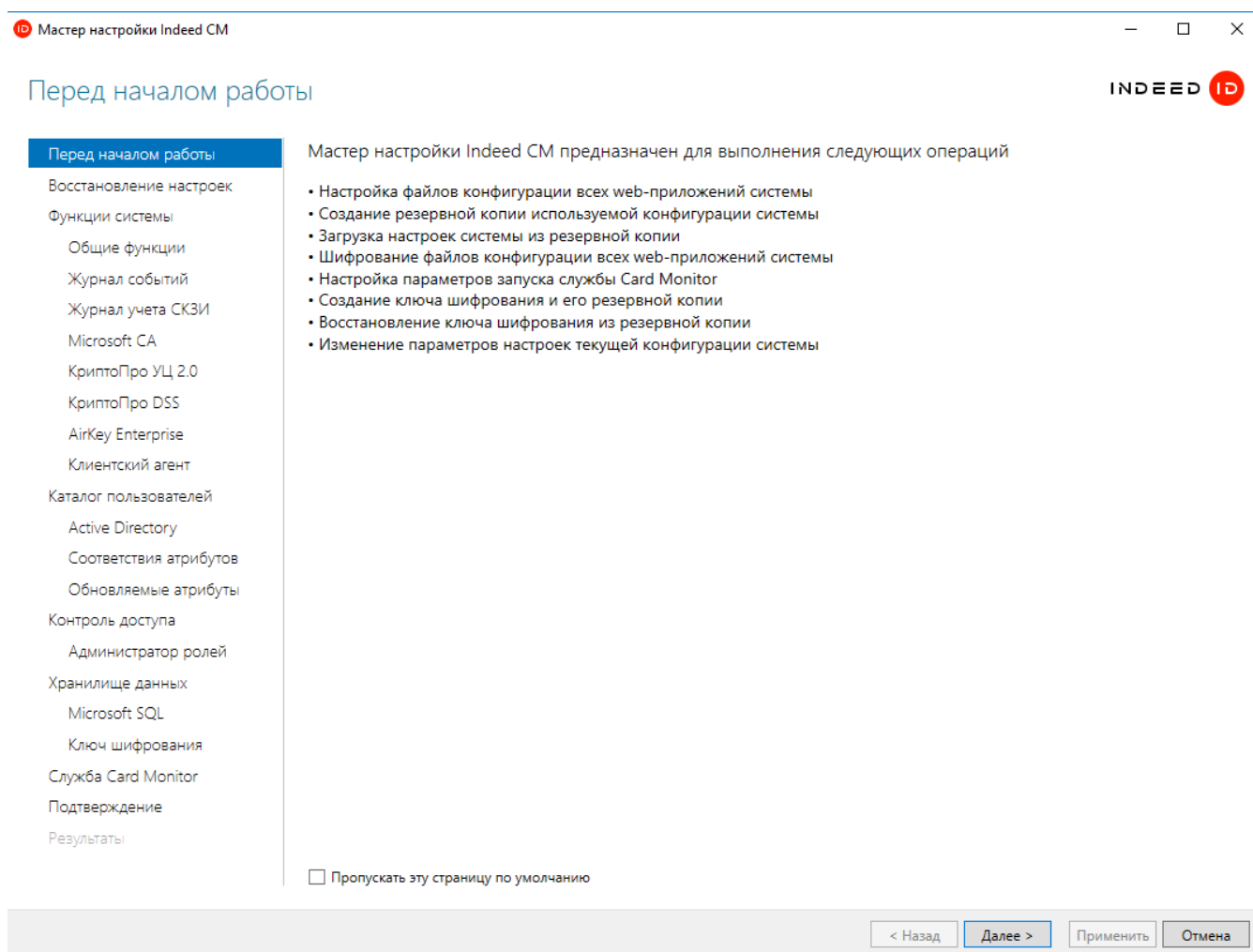







Рисунок 13 – Мастер настройки Indeed CM.

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: <ul style="list-style-type: none"> Общие функции Журнал событий Журнал учета СКЗИ Microsoft CA КриптоПро УЦ 2.0 КриптоПро DSS AirKey Enterprise Клиентский агент 	<p>Общие функции: настройка внутренних параметров web-приложений Indeed CM.</p> <ul style="list-style-type: none"> 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 <div style="border: 1px solid red; padding: 5px; margin-top: 10px;">  Журнал учета реализован только для конфигурации системы с использованием Хранилища данных в MS SQL. </div> <p>Журнал событий:</p> <ul style="list-style-type: none"> 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 <p>Журнал учета СКЗИ: настройка параметров ведения журнала учета СКЗИ.</p> <p>Удостоверяющие центры: настройка параметров работы с центрами сертификации.</p> <p>КриптоПро DSS: настройка интеграции с ПАК КриптоПро DSS.</p> <p>AirKey Enterprise: настройка интеграции с сервером виртуальных смарт-карт Indeed AirKey Enterprise.</p> <p>Клиентский агент: настройка параметров работы клиентского агента Indeed CM.</p>
Каталог пользователей: <ul style="list-style-type: none"> Active Directory КриптоПро УЦ 2.0 Active Directory + КриптоПро УЦ 2.0 	<p>Определение каталога пользователей системы. Параметры подключения отображаются в зависимости от выбранного каталога.</p>

Соответствия атрибутов	<p>Определение атрибутов, с которыми необходимо создать нового пользователя в Центре Регистрации КриптоПро УЦ 2.0 с использованием Indeed CM в момент выпуска устройства.</p> <p>Например: создать нового пользователя в ЦР КриптоПро с теми значениями атрибутов, которые есть для существующего пользователя Active Directory.</p>
Обновляемые атрибуты	<p>Определение списка атрибутов пользователя при изменении которых необходимо обновление сертификата.</p> <p>В список отслеживаемых атрибутов пользователя в параметрах шаблонов сертификатов Microsoft CA и КриптоПро УЦ 2.0 по умолчанию включены:</p> <ul style="list-style-type: none"> • Общее имя(CN) • E-mail • UPN-имя пользователя <div data-bbox="432 734 1436 896">  Отслеживание изменений в атрибутах пользователей доступно для атрибутов указанных в полях Субъект (Subject) и Дополнительное имя субъекта (Subject Alternative Name) сертификата. </div>
Контроль доступа: <ul style="list-style-type: none"> • Администратор ролей 	<p>Определение параметров доступа к сервисам Indeed CM.</p> <p>Определение учетной записи для первоначальной настройки привилегий пользователей в разделе Роли Консоли управления Indeed Certificate Manager.</p> <div data-bbox="432 1111 1436 1196">  Указанная учетная запись должна входить в каталог пользователей системы. </div>
Хранилище данных: <ul style="list-style-type: none"> • Active Directory или Microsoft SQL • Ключ шифрования 	<p>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.</p>

Служба Card Monitor	<p>Служба Card Monitor предназначена для выполнения операций по контролю за обращением смарт-карт и выполняет:</p> <ul style="list-style-type: none"> ○ 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 <div data-bbox="523 495 1439 613" style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p> Если обновление устройства проводилось через Агент Indeed CM без автоматического одобрения сертификатов оператором УЦ.</p> </div> <ul style="list-style-type: none"> ○ Рассылку почтовых уведомлений администраторам и пользователям системы: <ul style="list-style-type: none"> – 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 <div data-bbox="523 927 1439 1310" style="border: 1px solid #f00; padding: 5px; margin: 10px 0;"> <p> Для выполнения задач по регулярному запуску службы Card Monitor, учетная запись, указываемая в мастере настройки должна состоять в группе Администраторов (Administrators) на сервере Indeed CM и иметь разрешение на Вход в качестве пакетного задания (Log on as a batch job).</p> <p>Если для данной учетной записи изменился пароль, то для работы Card Monitor необходимо в Мастере настройки Indeed CM передобавить пользователя, указав новое значение пароля.</p> </div>
Подтверждение	<p>Сводная информация по настройкам всех разделов Мастера с возможностью создания резервной копии конфигурации Indeed CM.</p>
Результаты	<p>Прогресс работы Мастера по записи указанных значений в файлы конфигурации сервисов Indeed CM.</p>

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 КристоПро DSS
- Обновление устройства КристоПро DSS

- Отзыв устройства КристоПро DSS
- Удаление устройства КристоПро DSS
- Удаление AirKey



Если настроена интеграция с КристоПро 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.