Этот документ входит в комплект поставки продукта.
Информация, содержащаяся в этом документе, может быть изменена разработчиком без уведомления пользователя.

Контактная информация:

+7 (495) 640-06-09
Москва
+7 (812) 640-06-09
Санкт-Петербург

inbox@indeed-id.com
почта

8 800 333-09-06
support@indeed-id.com
техническая поддержка

Indeed Card Management

Руководство по эксплуатации

версия 5.0.0

Содержание

Введение

Приветствуем вас и благодарим за приобретение программных продуктов нашей компании. Это руководство поможет вам ознакомиться с принципом работы системы **Indeed CM** и её возможностями.

Условные обозначения

В Руководстве используются следующие условные обозначения:

Важная информация
Указания, требующие особого внимания при развертывании, настройке, работе или обновлении продукта.

Дополнительная информация
Указания, способные упростить развертывание, настройку, работу или обновление продукта.

Консоль управления Indeed CM

Общие сведения

Взаимодействие операторов и администраторов с системой осуществляется через веб-интерфейс. Настройка параметров системы и управление жизненным циклом устройств осуществляется при помощи web-приложения **Management Console** (Консоль администратора).
Приложение доступно по адресу *https://<адрес сервера Indeed CM>/icm*. Аутентификация в приложении осуществляется в соответствии с выбранной на этапе развертывания системы конфигурацией.
Рядовые пользователи имеют доступ к приложениям **Self Service** (Личный кабинет пользователя) и **Remote Self Service** (Удаленный личный кабинет пользователя), где могут управлять своими устройствами самостоятельно.

Настройка Indeed CM

Прежде, чем начать работу в системе, необходимо выполнить следующие действия:

- Добавить файл лицензии в систему
- Добавить необходимые типы устройств
- Выполнить настройку политик использования устройств

Процесс добавления лицензий и типов устройств, а также установки необходимых настроек описан в разделе **Конфигурация** приложения Management Console.

Конфигурация

Раздел предназначен для администраторов системы. Позволяет управлять лицензиями, типами и политиками использования устройств.

Управление лицензиями

Для добавления новой лицензии перейдите в меню **Лицензии**, нажмите **Добавить лицензию**, укажите файл лицензии и нажмите **Добавить** (Рисунок 1).

Рисунок 1 – Добавление лицензии Indeed CM.

После добавления лицензии информация по всем имеющимся лицензиям будет отображена в виде таблицы (Рисунок 2).

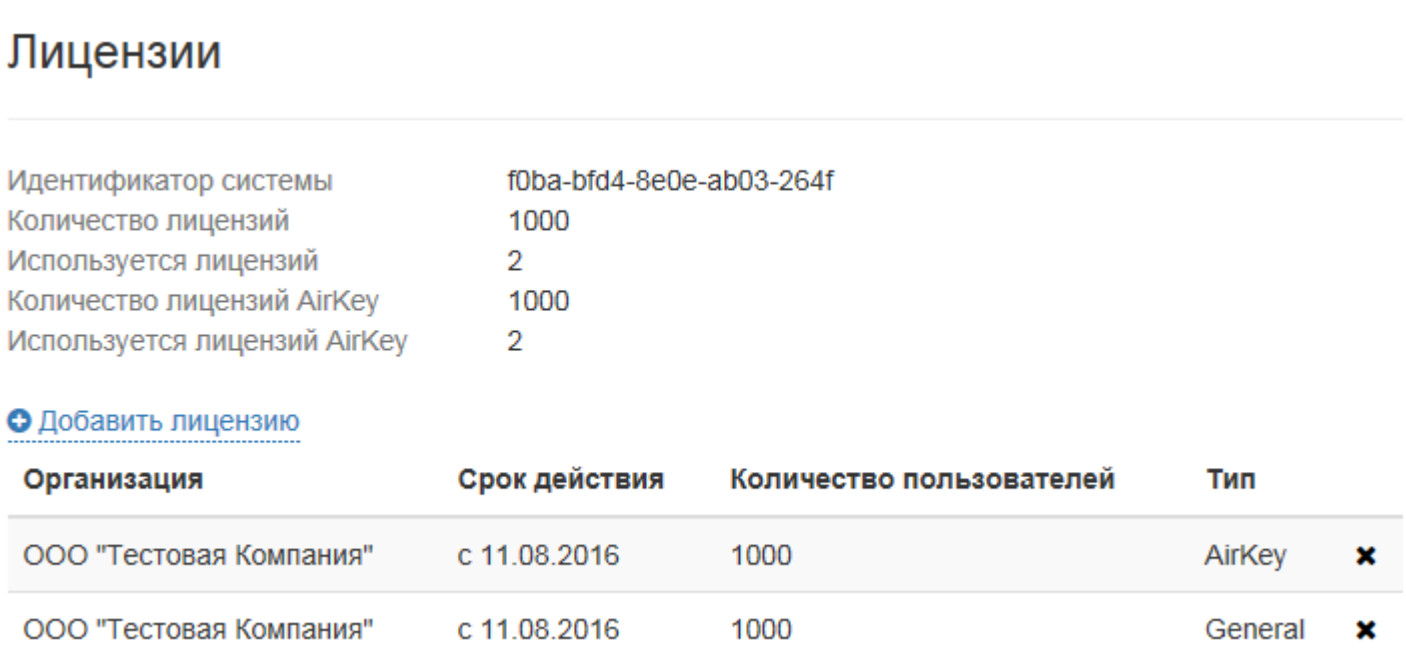

Рисунок 2 – Сведения о лицензиях Indeed CM и Indeed AirKey Enterprise.

Чтобы удалить лицензию из системы, выберите её в списке и нажмите ✖. Подтвердите действие нажатием кнопки **Удалить** (Рисунок 3).

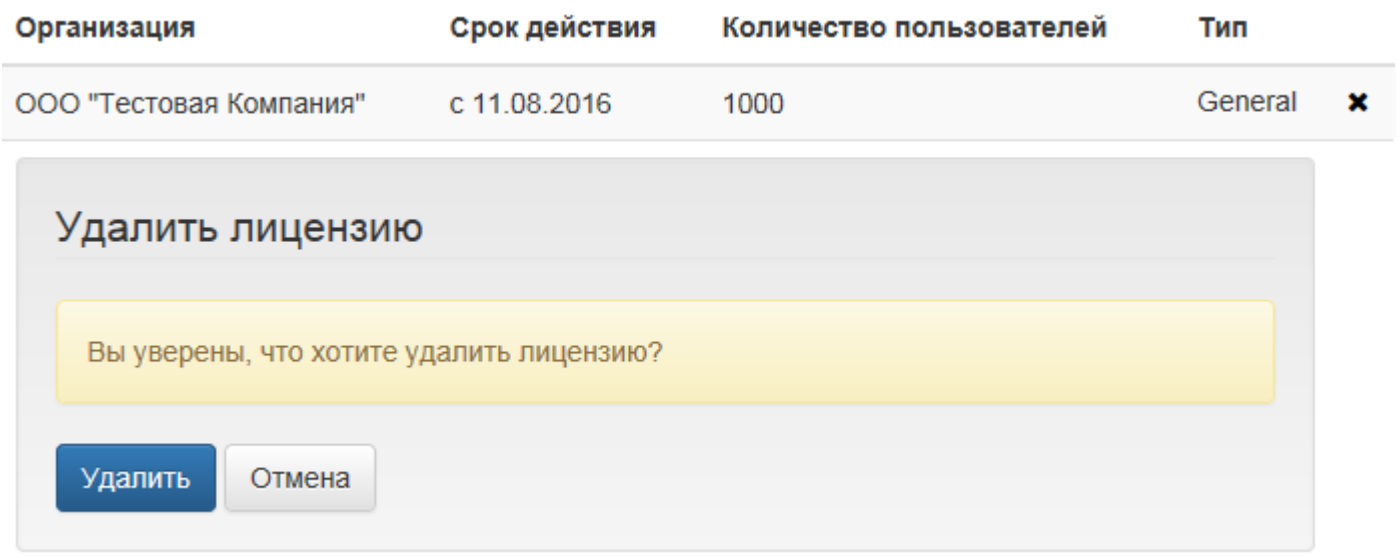

Рисунок 3 – Удаление лицензии Indeed CM.

Управление типами устройств

Indeed CM поддерживает работу с usb-токенами, смарт-картами и комбинированными устройствами. Количество поддерживаемых устройств аутентификации и типов постоянно увеличивается. Если в вашей организации появились устройства нового типа, или наоборот, устройства одного типа перестали использоваться, потребуется внести соответствующие изменения в Indeed CM.

Для добавления типа устройства перейдите в меню **Типы устройств**, нажмите **Добавить тип устройства**, укажите файл типа устройства и нажмите **Добавить**. Если необходимо заменить имеющийся в системе файл типа устройства, отметьте опцию **Заменить существующий** (Рисунок 4). Файлы для устройств различных типов поставляется вместе с дистрибутивом Indeed CM Server.

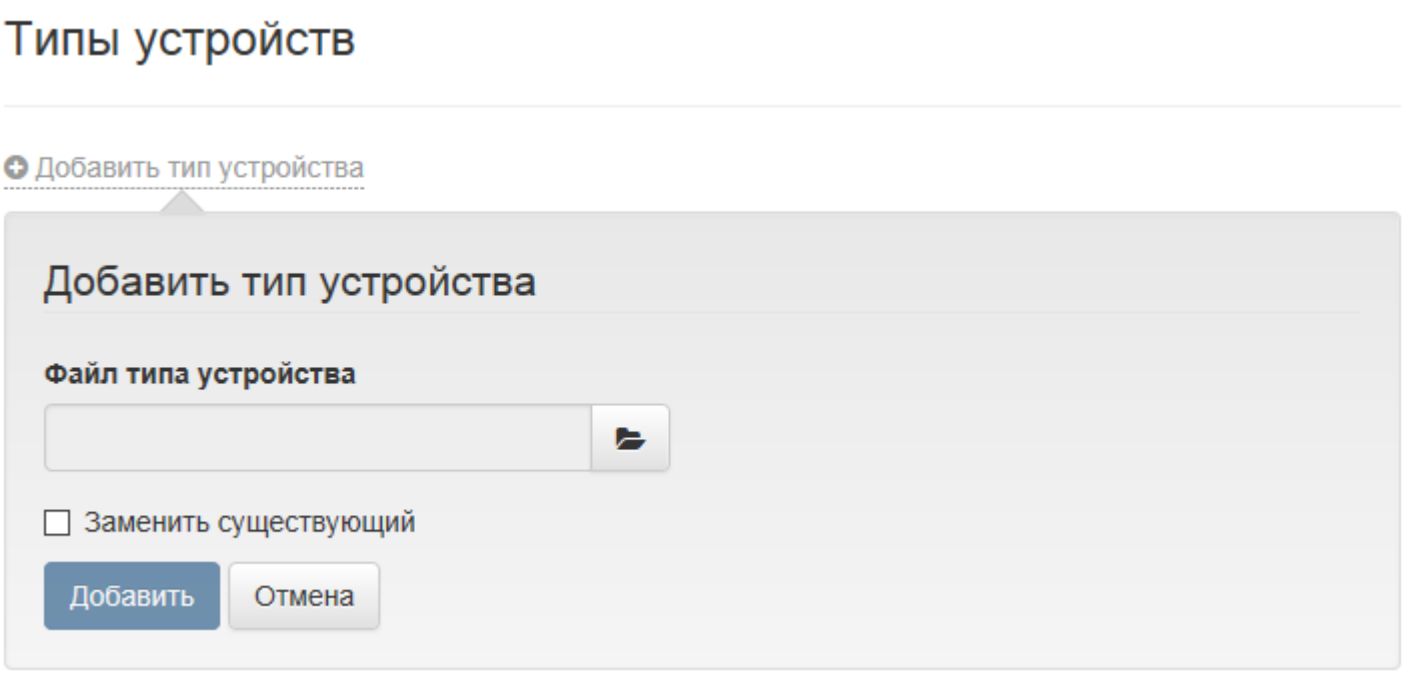

Рисунок 4 – Добавление типа устройства.

После добавления типа устройства в системе отобразится его имя (Рисунок 5).

Рисунок 5 – Добавленные типы устройств.

Файл типа устройства по умолчанию содержит предустановленные значения PIN-кодов администратора и пользователя (в том числе и для ГОСТ-области[1]). Эти значения могут быть изменены после добавления файла устройства в Indeed CM. Для редактирования типа устройства выберите нужный тип в списке и нажмите ✎, для просмотра PIN-кодов нажмите 👁 (Рисунок 6).

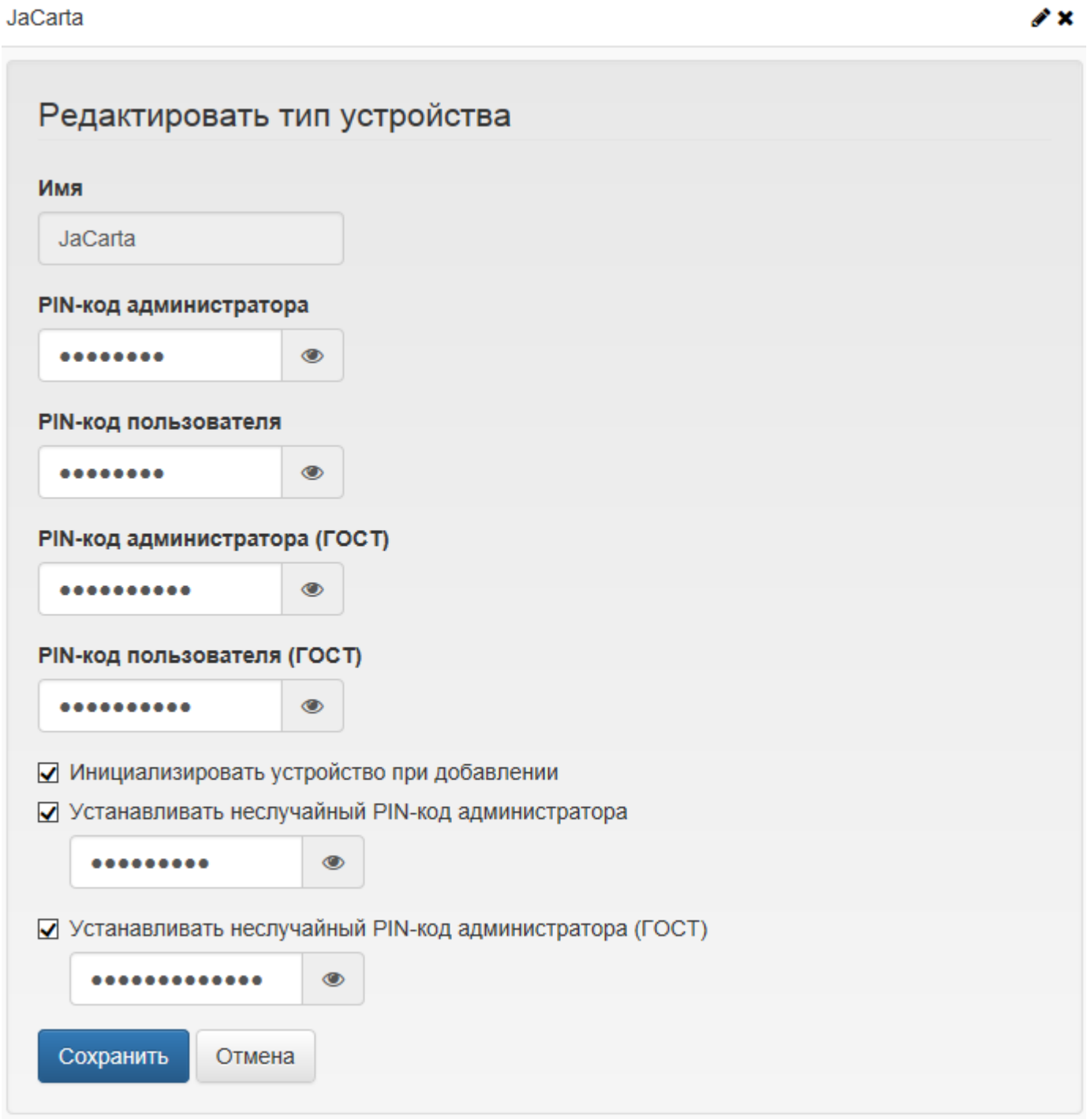

Рисунок 6 – Редактирование типа устройства.

[1]Наличие ГОСТ-области зависит от производителя и модели устройства.

При редактировании устройства доступны следующие опции:

- **Инициализировать устройство при добавлении** – Indeed CM позволяет выполнять инициализацию устройства в процессе добавления. При этом:
  - Добавляемое устройство будет очищено
  - В качестве имени устройства будет задано значение Empty
  - PIN-код администратора будет изменен на случайный (известный только Indeed CM) или указанный в опции **Установить неслучайный PIN-код администратора**
  - Количество попыток ввода PIN-кода администратора до блокировки будет равно 3
  - PIN-код пользователя, его минимальная длина и количество попыток ввода до блокировки будут изменены на указанные в файле типа устройства

  Для устройств eToken поддерживается инициализация с любым состоянием и значением PIN-кода администратора.

- **Устанавливать неслучайный PIN-код администратора** – если опция выключена, то при добавлении устройства установится случайный и известный только Indeed CM PIN-код. Если опция включена, то при добавлении устройства будет установлен указанный PIN-код.
- **Устанавливать неслучайный PIN-код администратора (ГОСТ)** – если опция выключена, то при добавлении устройства установится случайный и известный только Indeed CM PIN-код ГОСТ-области[2]. Если опция включена, то при добавлении устройства будет установлен указанный PIN-код для ГОСТ-области.

Для сохранения внесенных изменений нажмите **Сохранить**. Для удаления типа устройства, выберите его в списке, нажмите ✖ и подтвердите действие (Рисунок 7).

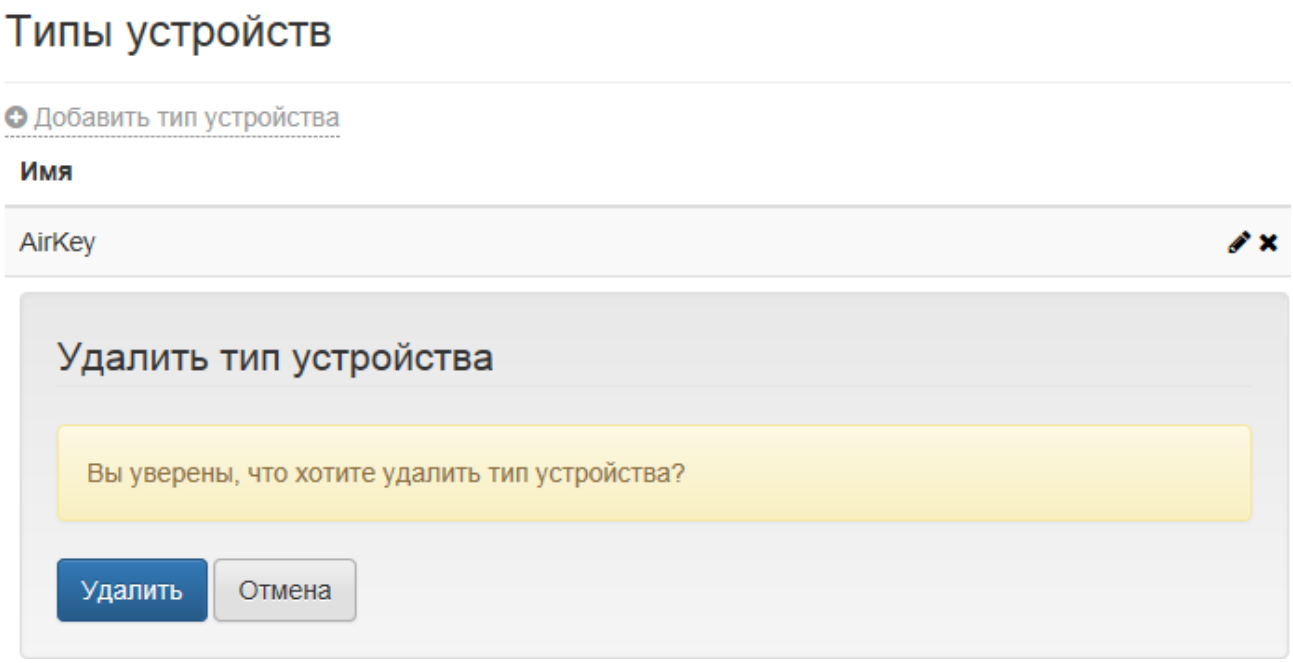

Рисунок 7 – Удаление типа устройства.

[2]Наличие ГОСТ-области зависит от производителя и модели устройства.

Организационная структура

Устройства в Indeed CM выпускаются пользователям по заданным правилам. Правила использования устройств, такие как необходимость инициализации, настройки выдачи, параметры аутентификации пользователей и т.д. задаются в политиках использования устройств, которые распространяются на указанную область. Область распространения политики – объект каталога пользователей. Например, подразделение домена Active Directory или папка в Центре Регистрации КриптоПро УЦ. Организационная структура позволяет объединить разрозненные объекты каталога пользователей под действие одной политики использования устройств.
На Рисунке 8 приведен пример организационной структуры. Для добавления нового узла нажмите **Добавить** и введите его имя. Для удаления созданного узла выберите его и нажмите **Удалить**. Для переименования узла щелкните по нему два раза левой кнопкой мыши или нажмите F2.

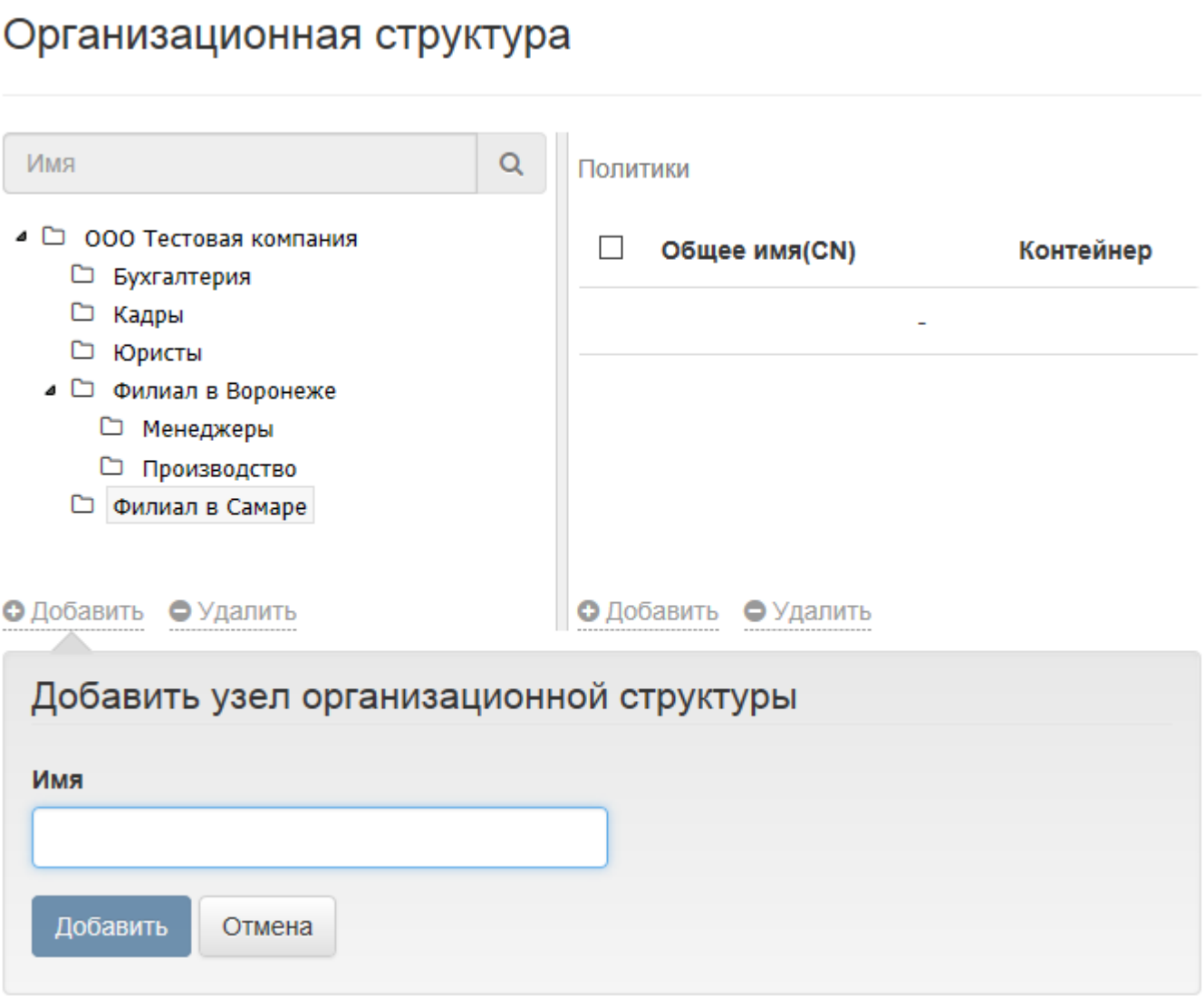

Рисунок 8 – Созданная организационная структура для назначения политик.

Для добавления объектов в узел нажмите **Добавить** в правой части окна редактирования организационной структуры. При создании структуры используются объекты каталога пользователей: контейнеры, подразделения и группы Active Directory, папки Центра Регистрации КриптоПро УЦ.

На Рисунке 9 приведен пример структуры организации, в узел которой добавлена группа пользователей Active Directory. Для добавления объекта в узел нажмите **Добавить**, укажите его тип и имя. Для удаления объекта выберите его и нажмите **Удалить**.

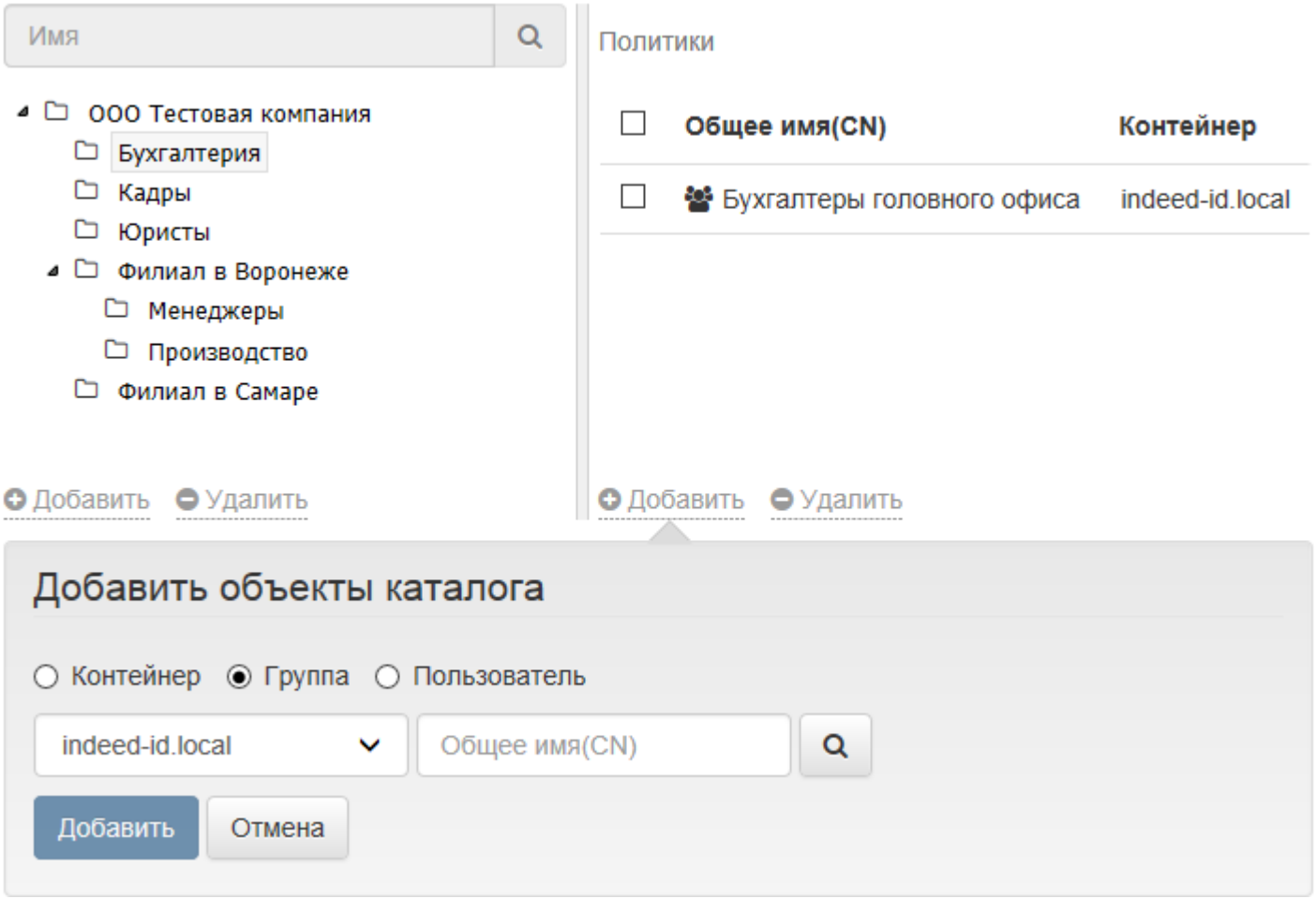

Рисунок 9 – Организационная структура с группой Active Directory в узле.

Назначенная на узел политика отображается в правой части окна (Рисунок 10).

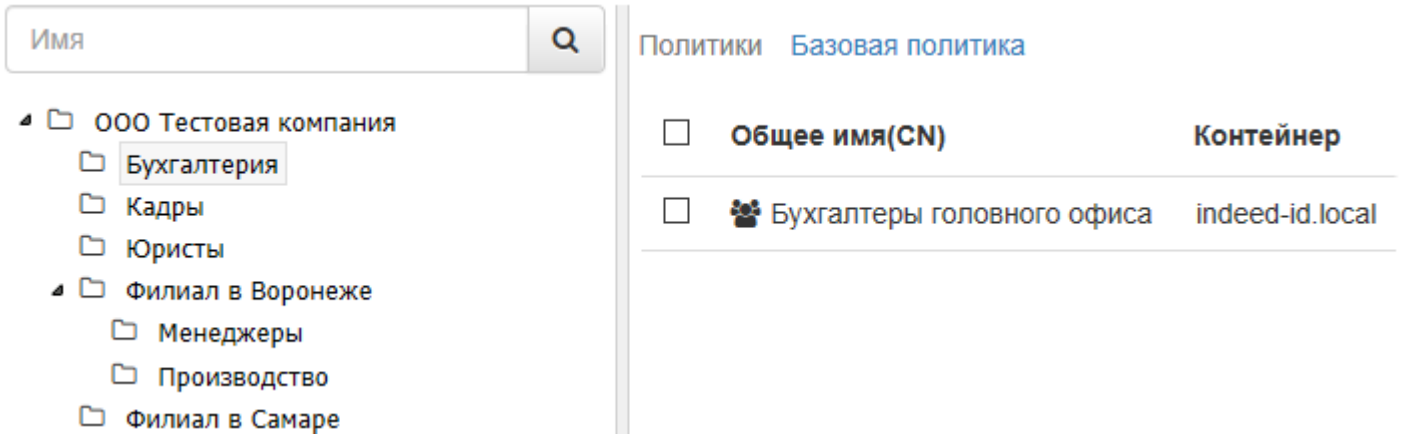

Рисунок 10 – Узел организационной структуры "Бухгалтерия" с назначенной Базовой политикой.

Политики

Создание и редактирование политик использования устройств осуществляется в меню **Политики** раздела **Конфигурация** в Management Console. В Таблице 1 приведены названия и описания политик использования устройств.

Таблица 1 – Названия и описания параметров политик использования устройств.

Группа политик	Описание
Общие	Сведения об имени и области действия политики.
Настройки PKI Microsoft[3] • Удостоверяющие центры • Шаблоны КриптоПро 2.0 • Удостоверяющие центры • Шаблоны	Настройки центров сертификации, шаблонов, параметров использования сертификатов, параметров доступа в операционную систему.
Общие сертификаты	Раздел для загрузки файлов PFX, содержимое которых должно записываться на устройства средствами Indeed CM.
Организации	Параметры организаций пользователей.
Indeed EA & ESSO	Параметры интеграции с продуктами Indeed Enterprise Authentication и Indeed Enterprise Single Sign-On.
Поведение	Параметры обращения с устройствами.
Контроль	Параметры контроля использования устройств пользователями.
Выпуск • Инициализация устройства	Настройки выпуска устройств и параметры инициализации.
Аутентификация • Секретные вопросы	Параметры аутентификации, создание и изменение секретных вопросов.
Принтер смарт-карт • Шаблон устройства	Настройки выпуска и печати на смарт-картах.
Уведомления • Группы получателей • Уведомления администратора • Уведомления пользователя • Шаблоны администратора • Шаблоны пользователя	Настройки почтовых уведомлений о событиях системы. Настройки шаблонов почтовых уведомлений.

[3]Отображение параметров того или иного удостоверяющего центра определяется на этапе настройки Indeed CM. См. раздел **Настройка параметров системы** в документе *Indeed CM. Руководство по установке и настройке*.

Для создания политики перейдите в меню **Политики** и нажмите **Создать политику** (Рисунок 11).

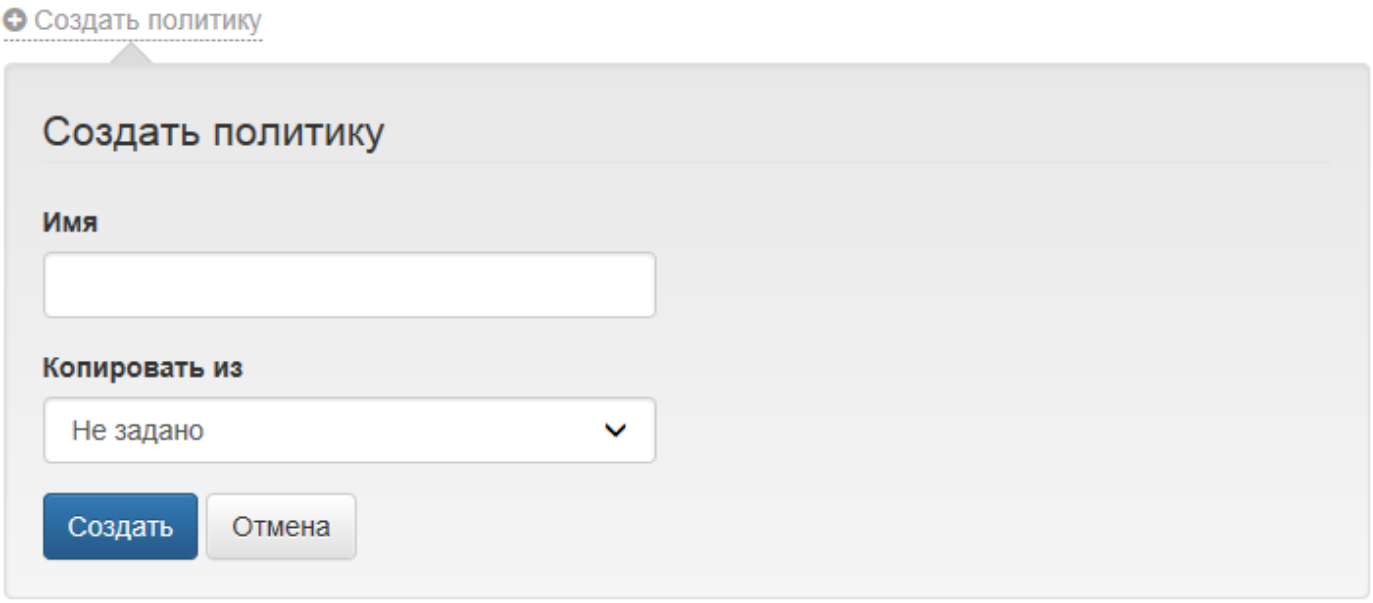

Рисунок 11 – Создание политики использования устройств.

Задайте:

- **Имя** – отображаемое имя политики
- **Копировать из** – создание новой политики через копирование параметров ранее созданной.

Нажмите **Создать**. После создания политики осуществится автоматический переход к её параметрам.

Общие параметры. В этом разделе отображается имя политики, которое можно изменить в случае необходимости. Для применения изменений нажмите **Сохранить**.

Настройки PKI. Раздел состоит из следующих пунктов:

- Настройки PKI
- Microsoft
  - Удостоверяющие центры
  - Шаблоны
- КриптоПро 2.0
  - Удостоверяющие центры
  - Шаблоны

На вкладке **Настройки PKI** настраиваются параметры входа в операционную систему:

Импортировать сертификаты УЦ
Определяет необходимость записи корневого сертификата удостоверяющего центра (или цепочки сертификатов) на устройство в момент выпуска. Такие сертификаты не удаляются с

Запись корневого сертификата или цепочки сертификатов может не поддерживаться устройством.

устройства при его изъятии из Indeed CM. Если опция включена, то корневые сертификаты или цепочки сертификатов будут записаны на устройство.

Требовать логон по смарт-карте[4]

Если опция включена, то в параметрах учетной записи пользователя в Active Directory при выпуске устройства будет применена настройка **Для интерактивного входа в сеть нужна смарт-карта** (Smart card is required for interactive logon).

Включение опции в профиле пользователя Active Directory приведет к тому, что его доменный пароль будет изменен на случайный и срок действия этого пароля будет неограничен (см. описание в статье Microsoft Общее представление об учетных записях пользователей).

Задайте необходимые параметры и нажмите **Сохранить**.

Microsoft. Вкладка содержит параметры работы с удостоверяющими центрами Microsoft. Чтобы добавить удостоверяющий центр, нажмите **Добавить УЦ** (Рисунок 12).

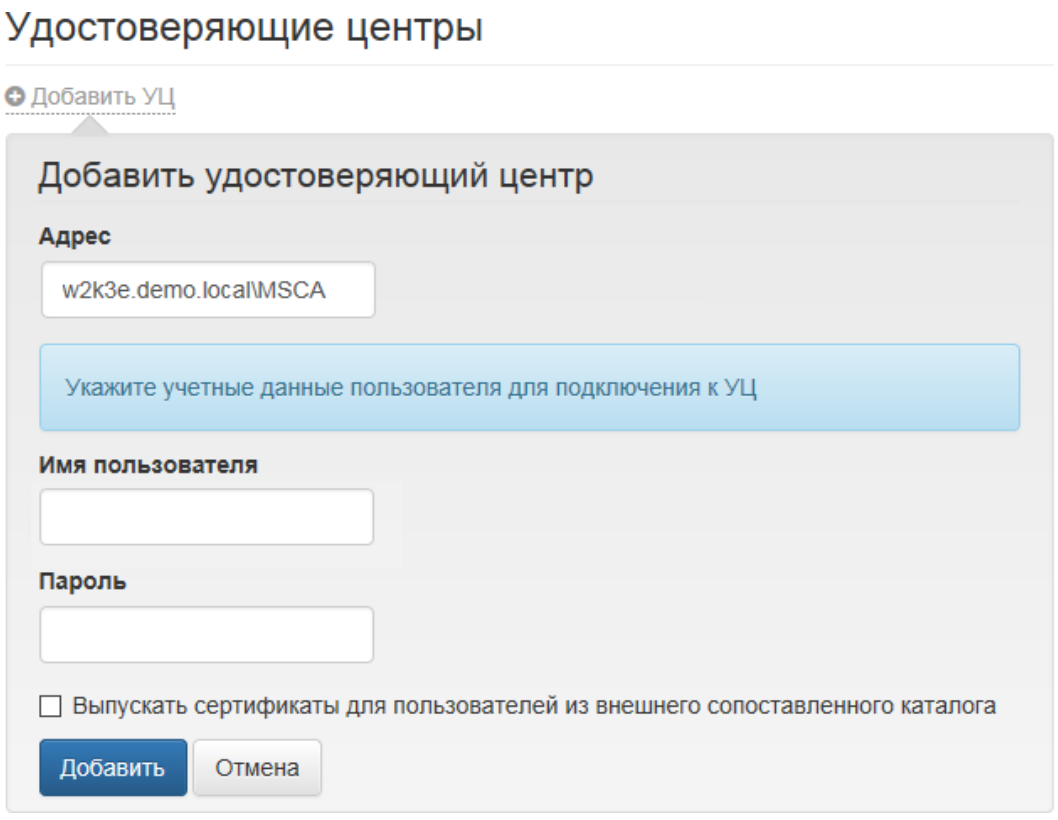

Рисунок 12 – Добавление удостоверяющего центра Microsoft.

[4]Только для каталога пользователей, расположенного в Active Directory (см. раздел **Настройка параметров системы** в документе *Indeed CM. Руководство по установке и настройке.pdf)*.

Задайте адрес удостоверяющего центра (если он не определился автоматически), укажите учетные данные пользователя, обладающего сертификатом **Агент регистрации** (Enrollment Agent), и нажмите **Добавить**.

Наличие пользователя с сертификатом Агент регистрации (Enrollment Agent) является обязательным условием для работы Indeed CM с УЦ. От имени этого пользователя будет выполняться запрос к указанному удостоверяющему центру на выдачу сертификатов пользователям Indeed CM. Учетные данные этого пользователя могут быть изменены после добавления удостоверяющего центра в Indeed CM (см. раздел **Работа с Microsoft Enterprise CA** в документе *Indeed CM. Руководство по установке и настройке.pdf)*.

Для изменения учетных данных пользователя, обладающего сертификатом **Агент регистрации** (Enrollment Agent), выберите нужный удостоверяющий центр и нажмите ✎ справа от имени пользователя. Для удаления удостоверяющего центра нажмите ✖.
Indeed CM поддерживает работу с множеством удостоверяющих центров организации. Вы можете добавить несколько УЦ для одной политики или создать несколько политик, указав для каждой свой удостоверяющий центр.

Для добавления удостоверяющего центра, расположенного за пределами домена в котором находятся пользователи Indeed CM (например, в другом независимом домене, который также принадлежит вашей организации) выполните следующие действия:

1. Нажмите **Добавить УЦ**.
2. В поле **Адрес** укажите URL-адрес приложения Indeed CM MSCA Proxy[5].

В случае развертывания Indeed CM в лесу доменов использование MSCA Proxy не обязательно. В этом случае в поле **Адрес** следует указать имя удостоверяющего центра.

3. Укажите учетную запись пользователя (в формате ДОМЕН\ИМЯ), обладающего сертификатом **Агент регистрации** (Enrollment Agent) на УЦ, расположенном вне домена с каталогом пользователей Indeed CM и её пароль.
4. Включите опцию **Выпускать сертификаты для пользователей из внешнего сопоставленного каталога**.
5. В поле **Путь (LDAP)** укажите путь к каталогу пользователей Indeed CM внешнего домена.

   Пример: Indeed CM развернут в домене demo.local и сертификаты пользователям этого домена выпускаются развернутым в этом домене УЦ. При добавлении УЦ, развернутого в домене demo2.local, следует указать путь к каталогу пользователей в этом домене, где у пользователей системы Indeed CM есть еще одна доменная учетная запись и на имя которой добавляемый УЦ будет выпускать сертификаты.

[5]См. раздел **Подключение к центру сертификации Microsoft через IndeedCM.MSCA.Proxy** в документе *Indeed CM. Руководство по установке и настройке.pdf*.

Таким образом, для одного сотрудника, имеющего учетные записи в независимых доменах, система позволит записать на одно устройство несколько сертификатов, выданных удостоверяющими центрами, расположенными в независимых доменах.

Выпуск сертификатов для пользователей внешнего каталога будет успешен только при совпадении атрибута соответствия с основным каталогом пользователей.
Например: адрес электронной почты, указанный в свойствах учетной записи пользователя в домене demo.local должен совпадать с адресом электронной почты, указанным в свойствах учетной записи пользователя в домене demo2.local.

6. В поле **Имя пользователя** укажите в формате ДОМЕН\ИМЯ учетную запись, обладающую правами на чтение всех свойств[6] пользователей во внешнем домене. Для этого можно использовать учетную запись, указанную в п.3.
7. В поле **Атрибут сопоставления каталогов** укажите атрибут, по которому Indeed CM будет определять уникальность пользователя, для которого созданы учетные записи в каждом домене. На Рисунке 13 приведен пример настроек для внешнего Microsoft CA.

[6]Для настройки разрешения на чтение только необходимого набора свойств обратитесь к разделу **Работа с Microsoft Enterprise CA** документа *Indeed CM.Руководство по установке и настройке.pdf*.

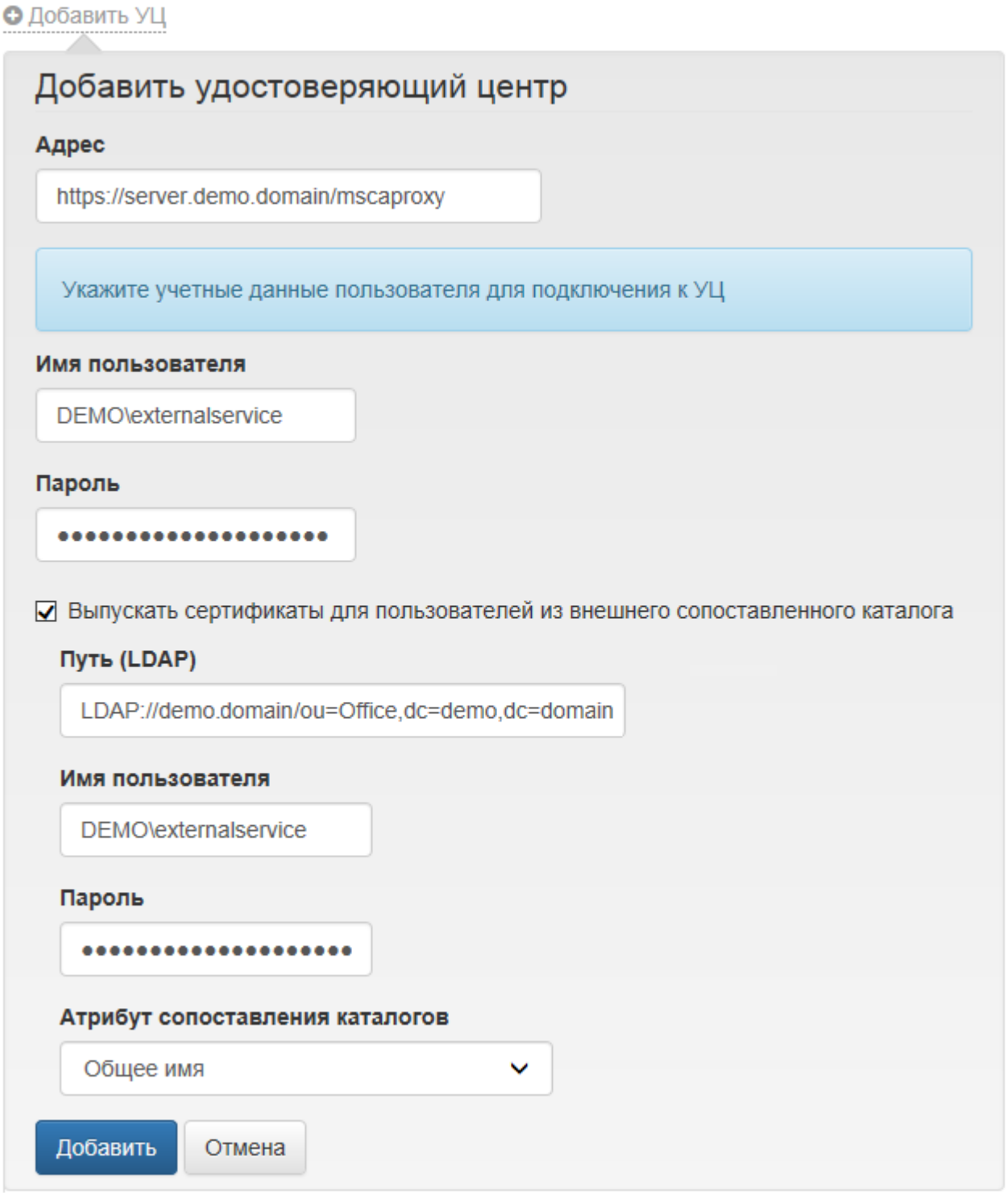

Рисунок 13 – Добавление УЦ Microsoft, расположенного вне каталога пользователей Indeed CM.

На вкладке **Шаблоны** задаются шаблоны, в соответствии с которыми будут выпускаться сертификаты пользователям.

Прежде, чем приступить к созданию шаблонов сертификатов в Indeed CM, убедитесь в том, что необходимые шаблоны добавлены в центр сертификации.

В разделе Параметры шаблонов сертификатов приведено описание настроек шаблонов сертификатов всех поддерживаемых в Indeed CM удостоверяющих центров.
Для создания шаблона сертификата нажмите **Создать шаблон сертификата**, задайте параметры шаблона (см. Таблицу 2) и нажмите **Создать**. Indeed CM позволяет создать множество разных шаблонов сертификатов для одной политики (при условии, что эти шаблоны не повторяются). Просмотреть список созданных шаблонов можно в разделе **Шаблоны** выбранной политики (Рисунок 14).

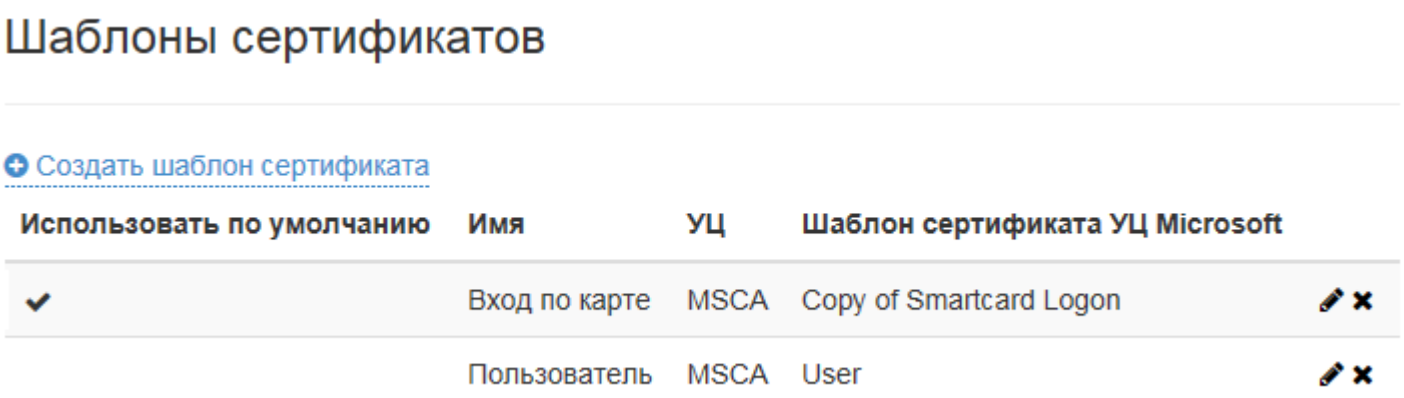

Рисунок 14 – Шаблоны сертификатов Microsoft CA.

Для редактирования шаблона выберите его и нажмите ✎. Для удаления шаблона из политики нажмите ✖.

КриптоПро 2.0. Вкладка содержит параметры работы с удостоверяющими центрами КриптоПро 2.0. В разделе **Удостоверяющие центры** задаются УЦ КриптоПро версии 2.0, с которыми будет работать Indeed CM. Чтобы добавить удостоверяющий центр, нажмите **Добавить УЦ** (Рисунок 15).

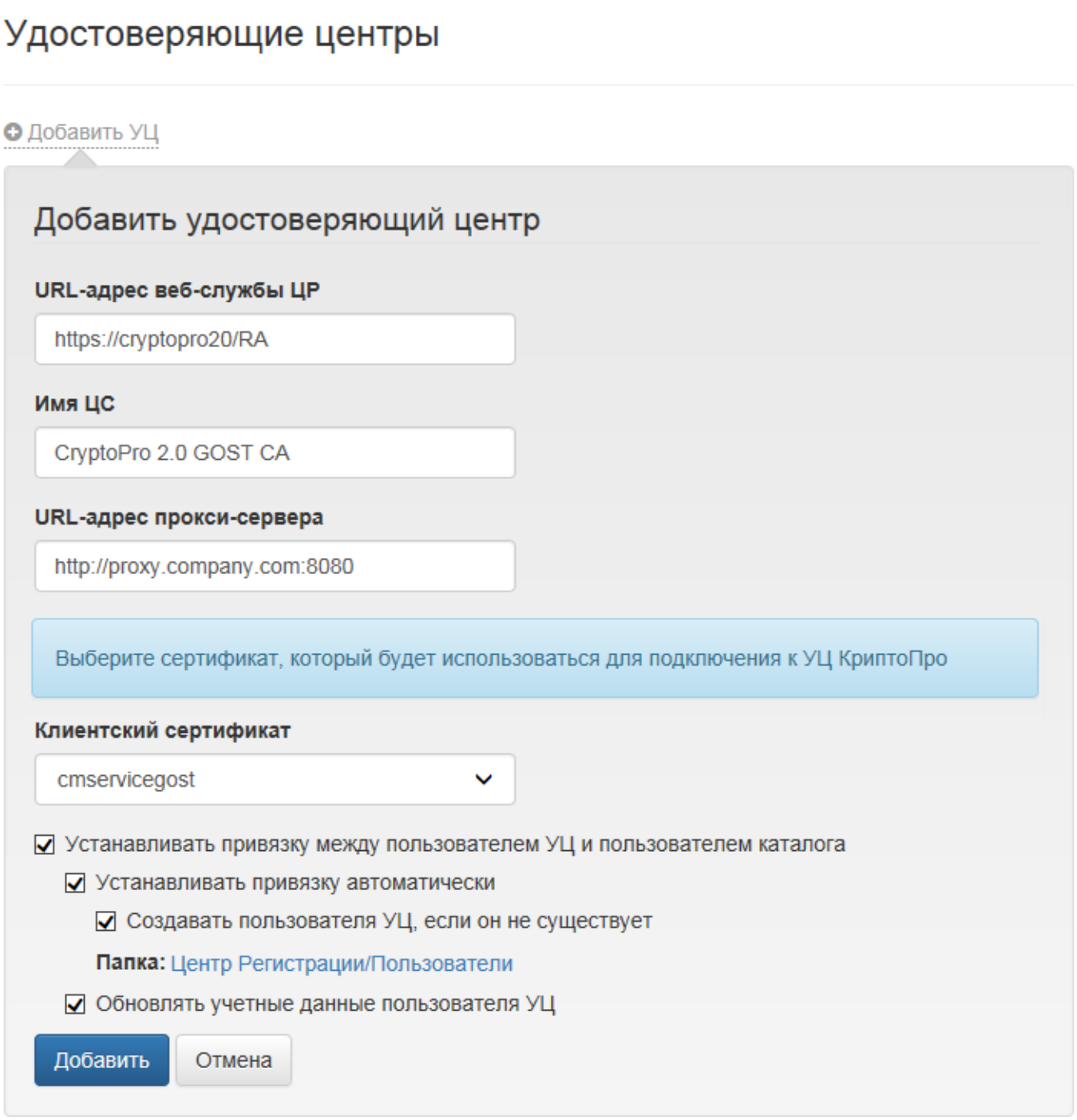

Рисунок 15 – Добавление удостоверяющего центра КриптоПро 2.0.

Введите **URL-адрес веб-службы Центра Регистрации**, в полном или сокращенном виде. **Например**:

https://<host name>/ra/RegAuthLegacyService.svc

https://<host name>/ra

Если для соединения с удостоверяющим центром используется прокси-сервер, укажите его параметры (имя сервера и порт) в поле **URL-адрес прокси-сервера**.

Пример: http://proxy.company.com:8080

Если на рабочей станции развернута только одна роль ЦС, то поле **Имя ЦС** можно оставить пустым (имя будет определено автоматически), если ролей ЦС несколько, задайте имя того ЦС, к которому необходимо подключиться.
Укажите имя пользователя, обладающего сертификатом **Indeed CM Service User** (см. раздел **Создание шаблона сертификата для сервисной учетной записи** в документе *Indeed CM. Руководство по установке и настройке*).

Установите связь между пользователями удостоверяющего центра КриптоПро и пользователями каталога, если это требуется (опция **Устанавливать привязку между пользователем УЦ и пользователем каталога**). Устанавливать связь между пользователями каталога и пользователями УЦ необходимо, если каталог пользователей системы Indeed CM не является каталогом пользователей УЦ. Такая ситуация может быть в следующих сценариях использования:

- Indeed CM работает с пользователями домена Windows, запрашивая для них сертификаты КриптоПро УЦ, который имеет свой каталог пользователей, не связанный с Active Directory.
- Indeed CM работает с пользователями КриптоПро УЦ, но таким пользователям необходимо кроме сертификатов «своего» УЦ выдавать еще и сертификаты одно или нескольких других удостоверяющих центров.

Indeed CM позволяет определять следующие параметры работы с УЦ, если опция **Устанавливать привязку между пользователем УЦ и пользователем каталога** включена:

- **Устанавливать привязку автоматически** (если каталог УЦ содержит пользователя, для которого будет выпущена карта)
- **Создавать пользователя УЦ, если он не существует** (если каталог УЦ не содержит пользователя, для которого будет выпущено устройство с сертификатом). По умолчанию пользователи будут создаваться в корневом каталоге Центра Регистрации (папка "Центр Регистрации"). Для создания пользователей во вложенных папках укажите имя папки.

Indeed CM может обновлять данные ранее созданных пользователей КритпоПро УЦ 2.0 при выпуске или обновлении устройства. Например, изменять email, если он изменился в профиле пользователя в Active Directory. Включите опцию **Обновлять учетные данные пользователя УЦ**, если обновление данных необходимо.

Для обновления данных должна быть установлена привязка пользователя Active Directory к пользователю Центра Регистрации. Если привязка не установлена, то в каталоге ЦР будет создан новый пользователь.

Indeed CM поддерживает работу с множеством удостоверяющих центров организации. Вы можете добавить несколько УЦ для одной политики или создать несколько политик, указав для каждой свой удостоверяющий центр.
На вкладке **Шаблоны** задаются шаблоны, в соответствии с которыми будут выпускаться сертификаты пользователям. В разделе Параметры шаблонов сертификатов приведено описание настроек шаблонов сертификатов всех поддерживаемых в Indeed CM удостоверяющих центров.
Для создания шаблона нажмите **Создать шаблон сертификата**, задайте нужные параметры шаблона (см. Таблицу 2) и нажмите **Создать**.

Параметры шаблонов сертификатов в Indeed CM. Параметры шаблонов поддерживаемых сертификатов приведены в Таблице 2.

Таблица 2 – Настройки шаблонов сертификатов в Indeed CM.

Параметр	Описание	MSCA	КП2.0
Имя	Имя шаблона сертификата.	+	+
УЦ	Имя удостоверяющего центра.	+	+
Шаблон сертификата	Загружается из выбранного удостоверяющего центра.	+	+
Префикс имени ключа	Если префикс не задан, то имя контейнера, содержащего ключевую пару, будет сформировано случайным образом. Если указан префикс, то он добавится перед именем контейнера. Значение префикса отображается в Indeed CM (имя контейнера в разделе СКЗИ) и в стороннем ПО для работы с контейнерами закрытого ключа (КриптоПро CSP, клиенты устройств и пр.). **Имя контейнера с префиксом может не поддерживаться устройством.**	+	+
Использовать аппаратную криптографию, если поддерживается	Если опция включена, то при выпуске сертификата ключевая пара будет создаваться с использованием криптографических алгоритмов, поддерживаемых устройством. Если устройство не поддерживает аппаратную криптографию, то будет использоваться КриптоПро CSP, установленный на рабочей станции, к которой подключено устройство. Изменить значение опции при редактировании шаблона нельзя.	-	+
Создать резервную копию ключа	Если опция включена, то ключи шифрования генерируются на сервере Indeed CM, сохраняются в хранилище системы и затем записываются на устройство. В случае замены устройства происходит запись сохраненных ключей на новое устройство. Если опция выключена, то ключ шифрования сразу генерируется на устройстве.	+	+
Разрешить экспорт ключа	Если опция включена, то закрытый ключ может быть экспортирован из хранилища на устройстве.	-	-
Записывать копию ключа при временной замене устройства	Если опция отключена, то копии сертификатов и закрытых ключей не будут записаны на временное устройство при замене. Если опция включена, то копии сертификатов и закрытых ключей будут записаны на временное устройство при замене, как и в случае с постоянной заменой.	-	+
Использовать ключи повторно	Если опция включена, то при обновлении сертификатов, записанных на устройство, существующий ключ шифрования будет использован повторно.	+	-
Импортировать ключ, если существует	Если опция включена, то система будет искать существующие ключи на устройстве (для указанного пользователя, УЦ и шаблона) и использовать их, не создавая новых ключей. Импорт ключа невозможен, если устройство будет инициализировано перед выпуском.	+	+
Отзывать сертификат при отзыве или выключении устройства	Если опция включена, то сертификаты пользователя будут отозваны при включении или отзыве устройства. Если опция выключена, то при выключении или отзыве устройства сертификаты не будут отозваны.	+	+

продолжение таблицы на следующей странице

Параметр	Описание	MSCA	КП2.0
Устанавливать сертификат в локальное хранилище	Если опция включена, то при выпуске (обновлении) устройства через Self Service записанные на него сертификаты добавятся в локальное хранилище пользователя на рабочей станции.	+	+
Публиковать сертификат в каталоге пользователей[7]	Если опция включена, то выпущенный сертификат опубликуется в профиле пользователя в Active Directory на вкладке **Опубликованные сертификаты** (Published Certificates). Сертификат удалится из профиля при включении опции **Удалять опубликованный сертификат при отзыве устройства**.	-	+
Публиковать сертификат в файловое хранилище	Если опция включена, то выпущенный сертификат будет помещен в сетевое хранилище (папку). При отзыве устройства сертификаты из хранилища не удаляются.	-	+
Публиковать сертификат в ЦФТ	Если опция включена, то выпущенный сертификат будет помещен в базу приложений ЦФТ. При отзыве устройства сертификаты из базы приложений ЦФТ не удаляются.	-	+
Публиковать список отозванных сертификатов	Если опция включена, то при выключении, включении и отзыве устройств будет выполняться внеочередная публикация списка отозванных сертификатов (CRL).	+	+
Автоматически одобрять запрос на сертификат	Если опция включена, то запросы на сертификат будут автоматически одобрены. Если опция выключена, то для завершения выпуска потребуется дождаться одобрения запроса на УЦ или отменить выпуск, если запрос будет отклонен.	+	+
Автоматически одобрять подписанный запрос на обновление сертификата	Если опция включена, то запрос на обновление сертификата будет одобрен автоматически. Если опция выключена, то для обновления сертификата потребуется дождаться одобрения запроса на УЦ.	+	+
Использовать по умолчанию	Если опция включена, то сертификат отмечается как используемый по умолчанию для входа в операционную систему Windows XP.	+	-
Выпускать сертификат на указанного пользователя	Если опция включена, то в свойствах шаблона отобразится поле поиска пользователя в каталоге ЦР КриптоПро УЦ, на которого будут выпускаться сертификаты. Отображение опции включается в Мастере настройки Indeed CM[8]. Изменить значение опции при редактировании шаблона нельзя.	-	+
Использовать комментарий устройства в качестве комментария пользователя к запросу на сертификат	Если опция включена, то в поле "Заметки пользователя" запроса сертификата будет добавлен текст комментария устройства.	-	+
Период обновления (дней)	Период времени, в течение которого сертификат и закрытый ключ можно обновить. Значение по умолчанию – 30 дней.	-	+
Необязательный сертификат	Если опция включена, то при выпуске устройства появится возможность выбора сертификатов для записи из числа отмеченных, как необязательные. Если опция выключена, то сертификат считается обязательным для записи на устройство.	+	+

[7]Только для каталога пользователей, расположенного в Active Directory.

[8]Опция "Отображать в параметрах шаблонов опцию выпуска сертификатов на указанного пользователя" в разделе **Функции системы**.

Общие сертификаты. Общие сертификаты используются в сценарии, когда уже выпущенный вне системы Indeed CM сертификат и закрытый ключ необходимо записать на устройства множества пользователей средствами Indeed CM.

Особенности работы системы с общими сертификатами:

- Поддерживаются сертификаты с ключами RSA и ГОСТ.
- Для записи ГОСТ-сертификатов требуется наличие КриптоПро CSP на сервере Indeed CM и рабочей станции, к которой подключено устройство.
- Общие сертификаты не могут быть приостановлены и отозваны, обновление возможно через удаление старого PFX и добавление нового.
- Общие сертификаты не публикуются в Active Directory, файловое хранилище и базу приложений ЦФТ, не помещаются средствами Indeed CM в хранилище сертификатов пользователя.
- Почтовые уведомления об истечении срока действия общих сертификатов не рассылаются

Для добавления общего сертификата в политику использования устройств выберите файл PFX, укажите пароль для доступа к содержимому файла и нажмите **Добавить**.

При включении опции **Необязательный сертификат** общий сертификат будет предлагаться к выбору для записи на устройство при его выпуске или обновлении. При отключенной опции сертификат будет записан на устройство без предоставления возможности выбора.

Организации. При создании пользователя в Центре Регистрации КриптоПро УЦ 2.0 Indeed CM использует данные из профиля пользователя Active Directory. Если в Active Directory отсутствует полная информация об организации пользователя (например: ОГРН, ИНН, полный адрес), то она может быть загружена из шаблона организации, настраиваемого в политике использования устройств Indeed CM.
Нажмите **Добавить организацию**, заполните необходимые поля и нажмите **Добавить** (Рисунок 16).

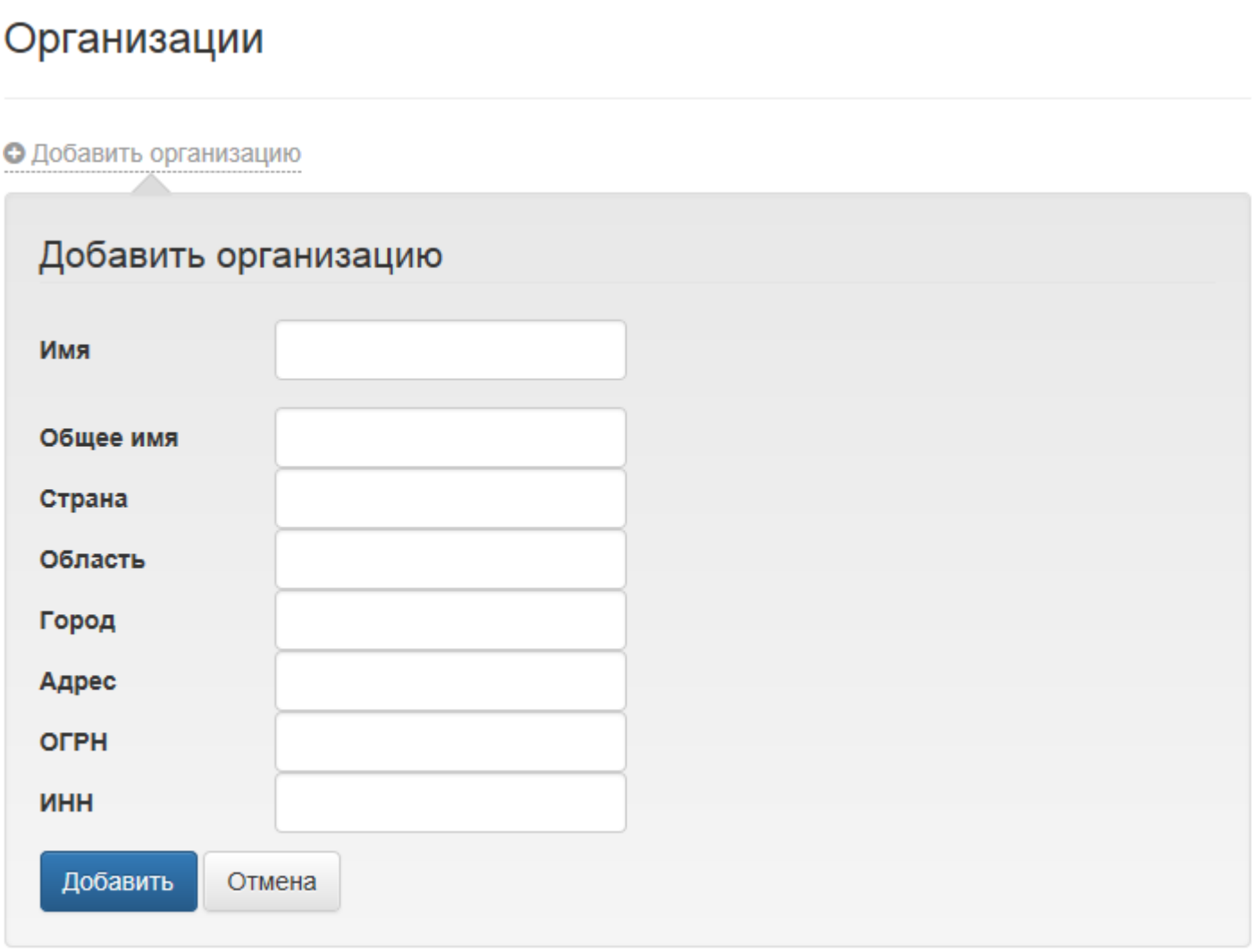

Рисунок 16 – Добавление организации пользователя.

Добавленные организации будут доступны администратору или оператору Indeed CM при выпуске карты пользователю, которого еще нет в каталоге Центра Регистрации КриптоПро УЦ 2.0. После выпуска устройства в каталоге ЦР будет создан пользователь, профиль которого будет заполнен данными из Active Directory (Общее имя, Фамилия, Имя, Отчество, email) и данными организации, выбранной из списка. При изменении данных в шаблоне организации данные в каталоге Центра Регистрации будут обновлены при следующем выпуске устройства. Для ранее созданных в каталоге ЦР пользователей данные по организации обновятся после обновления содержимого устройства.

Indeed EA & ESSO. Indeed CM может быть интегрирован с продуктами компании Индид – Indeed Enterprise Authentication и Indeed Enterprise Single Sign-On. Интеграция позволит объединить операции выпуска устройства, запроса сертификата, записи сертификата и регистрации аутентификатора в единый процесс.
Выпущенное подобным образом устройство может быть использовано пользователем как для аутентификации в домене и SSO-приложениях, так и для цифровой подписи или доступа к ресурсам, требующих наличие персональных сертификатов. Интеграция между системами возможна на любом этапе, независимо от того, какой из продуктов был развернут раньше.

Настройка интеграции систем Indeed Card Management и Indeed EA & ESSO состоит из двух этапов:

- Установка и настройка необходимого ПО
- Конфигурирование параметров интеграции

На первом этапе необходимо выполнить установку следующих компонентов:

- Indeed-Id Administration Tools (или Indeed-Id Admin Pack) на каждый сервер Indeed CM[9]
- Indeed-Id Extended Security Provider на каждый сервер Indeed EA[10]
- Indeed-Id SmartCard + PIN Provider на каждый сервер Indeed EA[11]

А также выполнить настройку Extended Security Provider:

- Создать группу безопасности Indeed-ID Enrollment Admins согласно Руководству по установке и эксплуатации Indeed-Id Extended Security Provider.
- Добавить сервисную учетную запись ('servicecm') в группы безопасности Indeed-ID User Admins и Indeed-ID Enrollment Admins.

На втором этапе необходимо задать параметры интеграции в политике использования устройств в Indeed Card Management. Перейдите в раздел **Indeed EA & ESSO** в конфигурации выбранной политики и определите параметры работы с Indeed EA & ESSO (Таблица 3).

Таблица 3 – Параметры интеграции с Indeed EA & ESSO.

Параметр	Описание
Включить интеграцию с Indeed EA & ESSO	Если опция включена, то при выпуске устройства в системе Indeed CM будет выпускаться и аутентификатор «Смарт-карта или USB-ключ + PIN» в системах Indeed EA/ESSO.
Использовать прокси-сервер Indeed EA	Если опция включена, то Indeed CM будет обращаться к прокси-серверу Indeed EA, который направит запрос на серверы Indeed EA/ESSO. Использование прокси-сервера необходимо, если серверы Indeed CM располагаются за пределами домена, в котором установлена система Indeed EA/ESSO.
URL-адрес прокси-сервера	Адрес, по которому доступен Indeed EA Proxy Server.
Имя пользователя **Пароль**	Учетные данные пользователя (логин и доменный пароль), входящего в группы безопасности Indeed-ID User Admins и Indeed-ID Enrollment Admins.
Разрешить использование Enterprise Authentication	Если опция включена, то при выпуске устройства в Indeed CM пользователю будет разрешено использование технологии Indeed для аутентификации в домене при помощи компонента Indeed-Id Windows Logon.
Разрешить использование Enterprise SSO	Если опция включена, то при выпуске устройства в Indeed CM пользователю будет разрешено использование технологии Indeed для аутентификации в приложениях при помощи компонента Indeed-Id Enterprise SSO Agent.
Генерировать случайный пароль учетной записи Windows	Если опция включена, то при выпуске устройства в Indeed CM для пользователя будет установлена опция генерации случайного доменного пароля. В этом случае при истечении срока действия пароля новый пароль будет сгенерирован случайным образом и будет известен только системе Indeed EA.

[9]Поставляется в дистрибутиве системы Indeed-Id Enterprise Authentication.

[10]Поставляется по запросу службой технической поддержки компании Indeed Identity.

[11]Поставляется по запросу службой технической поддержки компании Indeed Identity.

Разрешения на использование Enterprise Authentication, Enterprise SSO и генерацию случайного пароля будут выключены в случае удаления последнего зарегистрированного аутентификатора пользователя.
Например, если у пользователя не было ни одного аутентификатора в системе Indeed EA и ни одной устройства в системе Indeed CM, то после выпуска устройства с настроенными параметрами интеграции у пользователя появится один аутентификатор («Смарт-карта или USB-ключ + PIN») в системе Indeed EA и одно устройство (например, eToken) в системе Indeed CM.

В случае удаления устройства в Indeed CM, удалится и аутентификатор в Indeed EA, а если других обученных аутентификаторов нет, отключатся и разрешения на использование Indeed Enterprise Authentication, Indeed Enterprise Single Sign-On и генерация случайного пароля (если хотя бы одна из этих опций была активна на момент отзыва).

Поведение. В этом разделе задаются настройки, определяющие действия с устройством в рамках политики использования устройств. Описание параметров раздела приведено в Таблице 4.

Таблица 4 – Настройки действий с устройством.

Опция	Описание	Значение по умолчанию
Добавлять устройство автоматически	Добавлять устройство в систему (если оно не было добавлено ранее) в момент выпуска или назначении устройства пользователю. Если опция выключена, то выпуск или назначение устройства, подключенного к компьютеру, но не добавленного в систему, запрещен.	**Отключена**
Разрешить сброс PIN-кода устройства	Разрешить администратору сбрасывать PIN-код пользователям устройств.	**Включена**
Разрешить офлайновую разблокировку	Позволяет разблокировать устройство пользователя при помощи администратора системы в случае, когда соединение между рабочей станцией пользователя и сервером Indeed CM отсутствует. Необходимым условием разблокировки устройства является знание пользователем ответов на секретные вопросы. Проверку ответов на секретные вопросы при разблокировке устройства в случае необходимости можно отключить (опция **Проверять ответы на секретные вопросы**).	**Включена**
Разрешить отмену обновления устройства	Позволяет администратору или оператору Indeed CM отменить обновление содержимого устройства пользователя.	**Включена**
Разрешить пользователю добавление устройства	Разрешить пользователю выпуск устройства, не добавленного в систему. Устройство будет добавлено автоматически в процессе выпуска. Опция работает только если включена опция **Добавлять устройство автоматически**.	**Отключена**
Разрешить пользователю назначение устройства	Разрешить пользователю выпуск устройства, не назначенного на него администратором.	**Отключена**
Разрешить пользователю отзыв устройства	Разрешить пользователю отзыв своего устройства.	**Включена**

продолжение таблицы на следующей странице

Опция	Описание	Значение по умолчанию
Разрешить пользователю включение устройства	Разрешить пользователю включение своего устройства (если оно было выключено ранее).	**Включена**
Разрешить пользователю выключение устройства	Разрешить пользователю выключение своего устройства (если оно была включено ранее).	**Включена**
Разрешить пользователю очистку устройства	Разрешить пользователю очистку содержимого своего устройства при его отзыве оператором с причинами **Изъятие устройства** и **Обновление устройства**. После очистки устройство останется назначенным пользователю.	**Отключена**
Разрешить пользователю сброс PIN-кода устройства	Разрешить пользователю сброс PIN-кода своего устройства.	**Отключена**
Разрешить пользователю обновление устройства	Разрешить пользователю обновлять сертификаты, хранящиеся на его устройстве, в случае, если их срок действия истек (или истекает).	**Включена**
Разрешить пользователю выбор необязательных сертификатов	Если опция включена, то при выпуске устройства в приложении Self Service пользователь сможет выбрать (среди необязательных сертификатов), те сертификаты, которые необходимо записать на устройство. Если опция выключена, то сертификаты, отмеченные в политике выпуска устройств, как необязательные, записаны на устройство не будут.	**Отключена**
Разрешить пользователю выпуск AirKey карты	Если опция включена, то пользователи смогут самостоятельно выпускать карты AirKey в приложении Self Service. Выпуск карт AirKey возможен только при настроенной интеграции с Indeed AirKey Enterprise (см. *Indeed AirKey Enterprise. Руководство по установке и эксплуатации.pdf*).	**Отключена**
Пользователь должен задать ответы на секретные вопросы при первом входе в сервис самообслуживания	Если опция включена, то после входа пользователя в приложение Self Service первый раз необходимо будет установить секретные вопросы и ответы на них. Вопросы в дальнейшем будут использоваться для аутентификации пользователя. Если опция выключена, то форма установки секретных вопросов при входе в сервис самообслуживания отображаться не будет. Пользователь сможет установить секретные вопросы позднее в любой момент.	**Включена**
Включить отслеживание сертификатов	Если опция включена, то при выпуске устройства Indeed CM выполнит поиск имеющихся на устройстве сертификатов и соответствующих им закрытых ключей. Поддерживается отслеживание сертификатов, выпущенных удостоверяющими центрами: • Microsoft CA • КриптоПро УЦ 2.0 • ViPNet УЦ 4 При скором истечении срока действия таких сертификатов Indeed CM может рассылать соответствующие почтовые уведомления.	**Отключена**

Контроль. Контроль за использованием устройств осуществляется при помощи клиентского Агента Indeed CM, устанавливаемого на рабочие станции пользователей. В разделе **Контроль** задаются действия и тексты сообщений (опционально), которые будут выполняться при нарушении правил использования устройств. Например, в случае подключения своей смарт-карты к рабочей станции другого пользователя. Описание параметров раздела приведено в Таблице 5.

Таблица 5 – Настройки использования устройства.

Опция	Описание
Сообщение пользователю при несовпадении привязанного устройства и агента	Сообщение, которое будет отображено пользователю Агентом Indeed CM при подключении устройства к неразрешенной администратором рабочей станции. Если значение не задано, то сообщение не будет отображаться.
Действие, выполняемое при несовпадении привязанного устройства и агента	Действие, которое будет выполнено Агентом Indeed CM при подключении устройства к неразрешенной администратором рабочей станции. Возможные варианты: • Без действия • Блокировка пользовательской сессии • Блокировка устройства • Блокировка пользовательской сессии и устройства
Включить привязку устройства к пользователю	Если опция включена, то Агент Indeed CM при подключении устройства к рабочей станции будет проверять его принадлежность к пользователю, под которым было выполнено подключение.
Сообщение пользователю при несовпадении привязанного устройства и пользователя	Сообщение, которое будет отображено пользователю Агентом Indeed CM при подключении устройства к рабочей станции с сессией другого пользователя. Если значение не задано, то сообщение не будет отображаться.
Действие, выполняемое при несовпадении привязанного устройства и пользователя	Действие, которое будет выполнено Агентом Indeed CM при подключении устройства к рабочей станции с сессией другого пользователя. Возможные варианты: • Без действия • Блокировка пользовательской сессии • Блокировка устройства • Блокировка пользовательской сессии и устройства
Таймаут до блокировки пользовательской сессии (сек.)	Период времени, по истечении которого сессия пользователя будет заблокирована, если блокировка выбрана как действие, которое должен выполнять Агент Indeed CM при нарушении правил использования устройства пользователем. Возможный интервал от 0 до 5 секунд.

Выпуск. В этом разделе задаются параметры выпуска устройства и параметры его инициализации. Описание параметров раздела приведено в Таблице 6.

Таблица 6 – Настройки выпуска устройства.

Опция	Описание
Максимальное количество устройств у пользователя	Число, ограничивающее количество устройств у пользователя. Значение по умолчанию – 1.
Инициализировать устройство	Если опция включена, устройство будет инициализировано перед выпуском. В результате инициализации все данные, хранящиеся на устройстве, будут удалены.

продолжение таблицы на следующей странице

Опция	Описание
Установить случайный PIN-код пользователя	Если опция включена, то в процессе выпуска устройства будет установлен случайный PIN-код пользователя. При включении опции становятся доступными для редактирования **Параметры генерации PIN-кода пользователя**: • Использовать только цифры • Длина (от 4 до 31 символа)[12] • Отображать установленный PIN-код администратору • Отображать установленный PIN-код пользователю Формируемый случайный PIN-код соответствует следующим правилам: • Содержит латинские строчные буквы • Содержит латинские прописные буквы • Содержит цифры • Повторы любых символов запрещены Случайный PIN-код пользователя может быть сообщен сотруднику, выпускающему карту. Случайный PIN-код пользователя может быть сообщен пользователю или его руководителю посредством почтового уведомления (см. Уведомления). Если в разделах **Выпуск** и **Инициализация устройства** будут указаны разные значения длины PIN-кода пользователя, то в процессе выпуска устройства будет использовано большее из них.
Пользователь должен поменять PIN-код при первом входе	Если опция включена, то пользователю будет необходимо изменить PIN-код устройства при первом его подключении к рабочей станции. **Опция поддерживается только устройствами eToken и JaCarta PKI**. Данная опция и опции **Устанавливать случайный PIN-код пользователя** и **Блокировать устройство** взаимоисключаемы.
Блокировать устройство	Если опция включена, то устройство будет заблокировано после выпуска. Перед использованием устройства, пользователь должен будет его разблокировать любым доступным способом (в режиме online или offline) и установить новый PIN-код.
Генерировать имя устройства автоматически	Если опция включена, то в качестве имени устройства может быть использовано одно из следующих значений из свойств пользователя: • Общее имя (CN) • Логин • Фамилия • E-mail • Подразделение • Заданная строка Выбранное значение будет автоматически подставлено в имя устройства в окне выпуска. При включенной опции **Разрешить редактирование имени устройства** подставленное имя может быть изменено сотрудником или пользователем перед выпуском устройства.

Параметры инициализации устройств. На вкладке **Инициализация устройства** задаются параметры инициализации для каждого типа устройств, поддерживаемых в Indeed CM.

[12] Длина случайного PIN-кода зависит от настройки **Минимальная длина PIN-кода** пользователя на вкладке **Инициализация устройства**.

Параметры инициализации, задаваемые в интерфейсе Indeed CM (требования к длине и сложности пароля, количество попыток ввода до блокировки и т.д) будут сохранены на устройстве до следующей инициализации.
Для настройки инициализации нажмите **Добавить параметры инициализации** и выберите тип устройства (Рисунок 17).

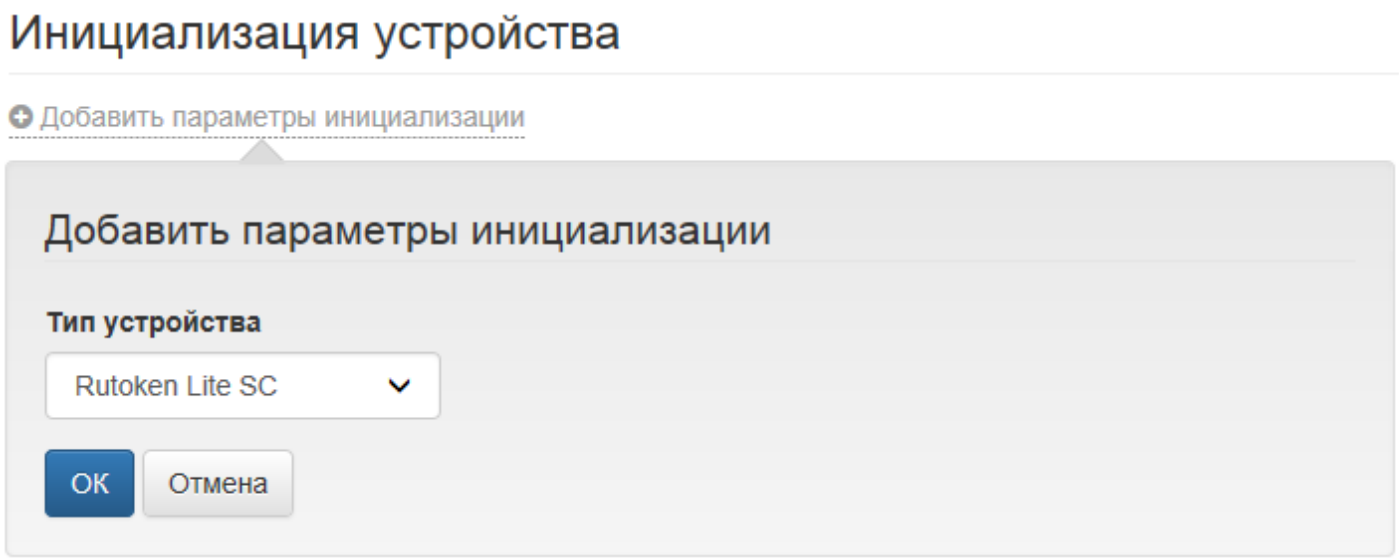

Рисунок 17 – Добавление параметров инициализации для выбранного типа устройства.

Если устройство не поддерживает настраиваемые парольные политики, то в процессе его инициализации можно установить только PIN-код пользователя (Рисунок 18).

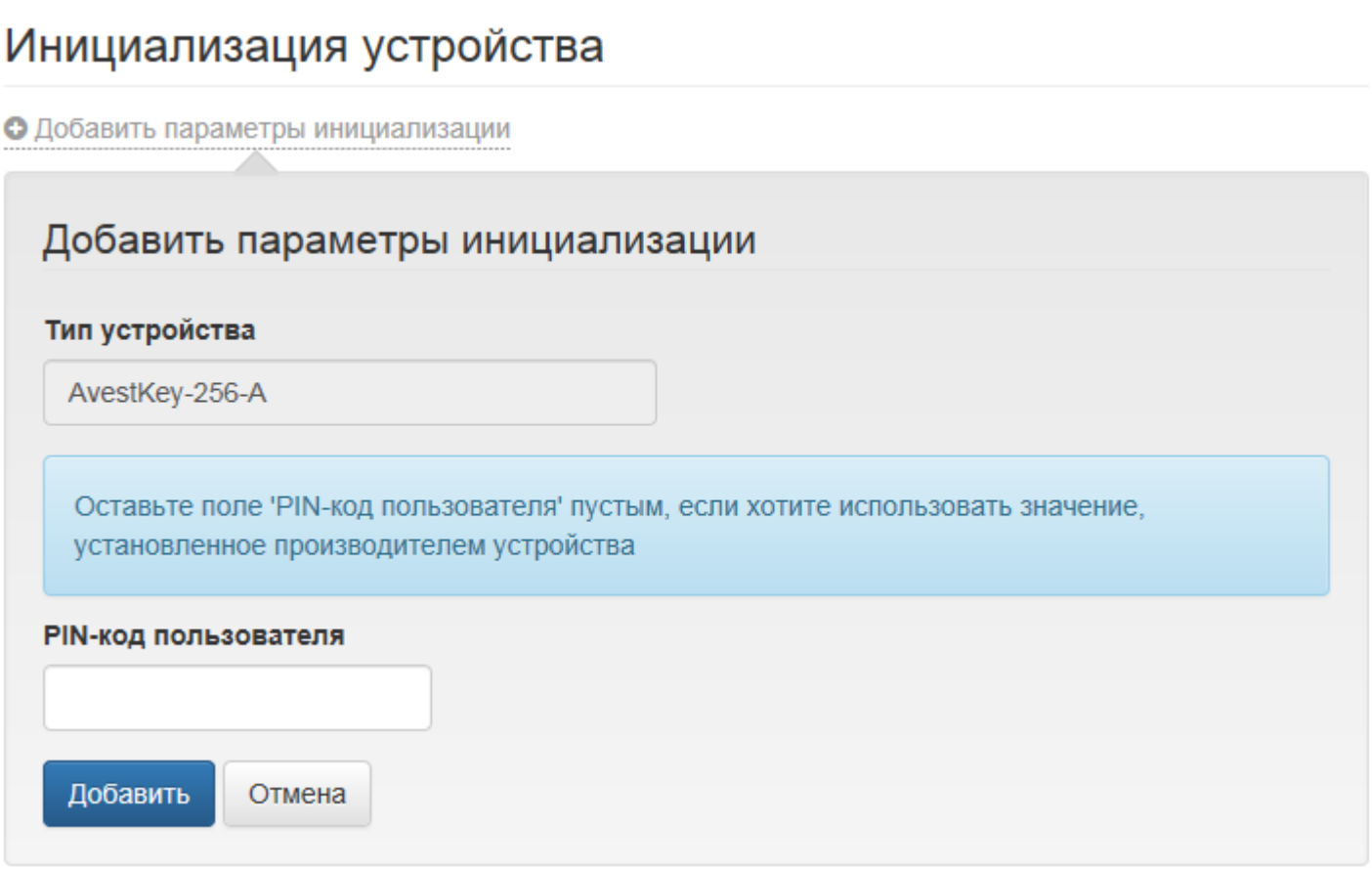

Рисунок 18 – Параметры инициализации устройства, не поддерживающего хранение парольных политик.

В этом случае всем пользователям, на которых распространяется политика, будут выпускаться устройства с заданным PIN-кодом.

Параметр **PIN-код пользователя** может быть пустым, в этом случае будет использован PIN-код, установленный производителем устройства по умолчанию.

Если устройство поддерживает настраиваемые парольные политики, то в зависимости от модели и производителя будет отображен список доступных для изменения параметров (Рисунок 19).

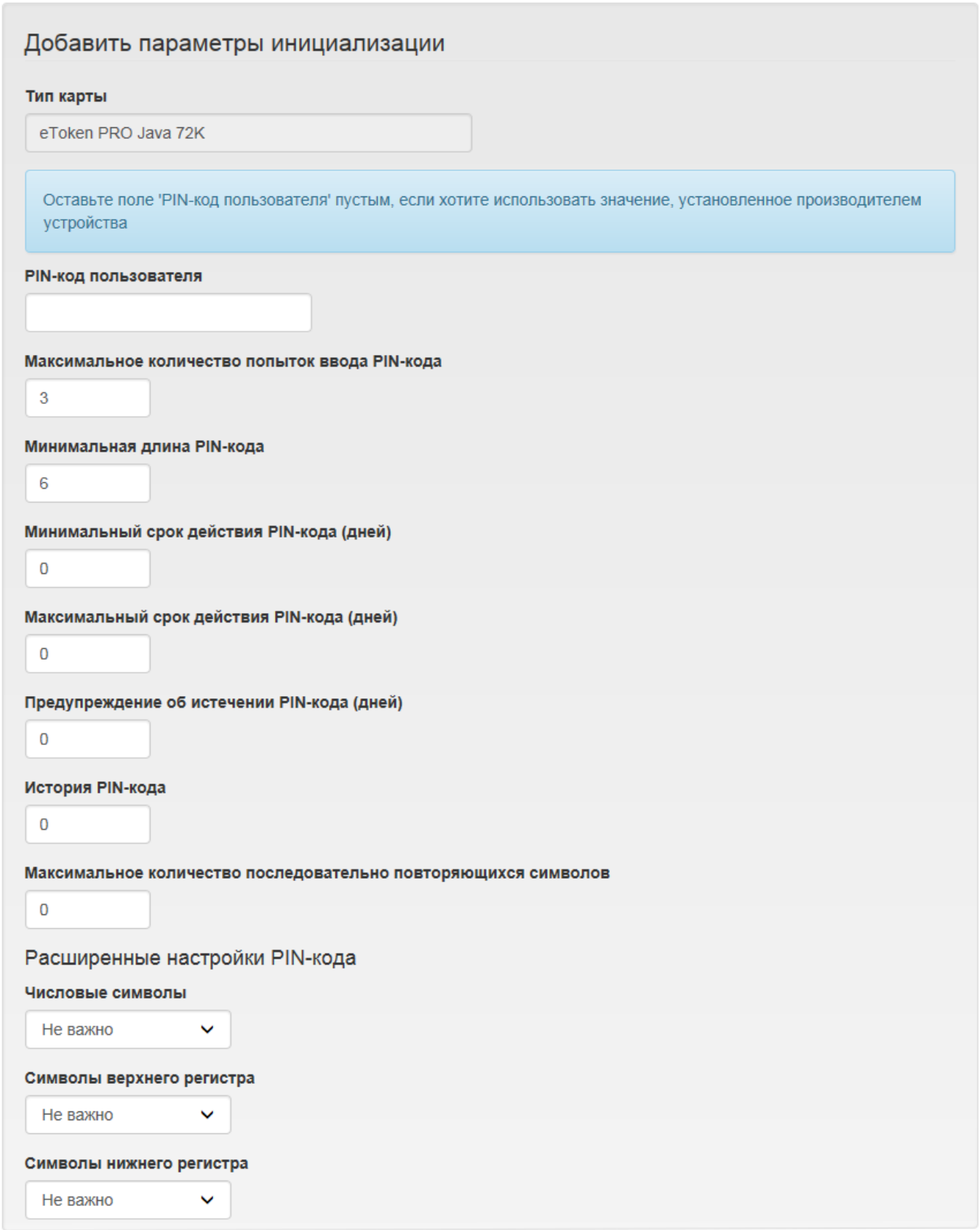

Рисунок 19 – Параметры инициализации устройства с поддержкой парольных политик.

Установите параметры инициализации и нажмите **Добавить** для сохранения. Параметры инициализации для каждого типа устройства можно изменить или удалить. Для редактирования параметров нажмите ✎. Для удаления нажмите ✖ (Рисунок 20).

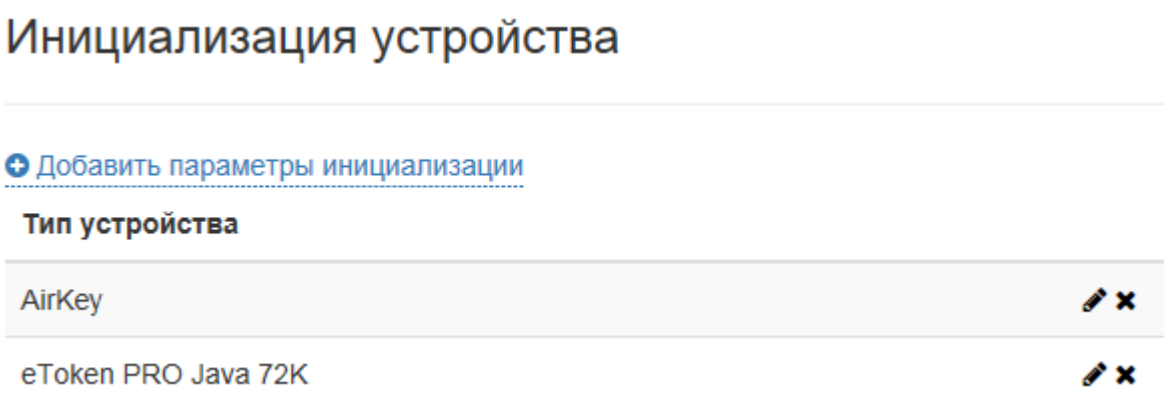

Рисунок 20 – Добавленные в политику выпуска устройств параметры инициализации.

В случае отсутствия в политике параметров инициализации для любого выпускаемого устройства при включении инициализации будут установлены значения по умолчанию (см. Управление типами устройств).

Аутентификация. Аутентификация пользователей осуществляется при разблокировке устройства, выключении устройства без выполнения входа в ОС и при доступе в сервис самообслуживания Remote Self Service. В этом разделе задаются параметры аутентификации пользователей: количество секретных вопросов (значение по умолчанию – 2) и максимальное количество попыток аутентификации по секретным вопросам до блокировки пользователя (значение по умолчанию – 3), Рисунок 21.

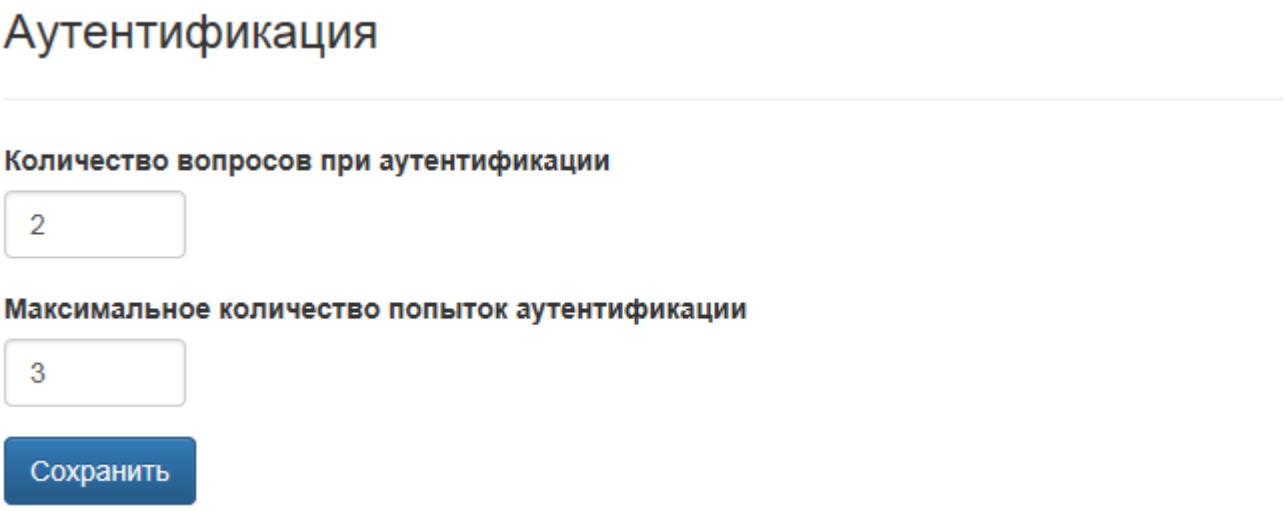

Рисунок 21 – Параметры аутентификации пользователей.

На вкладке **Секретные вопросы** задаются параметры секретных вопросов: список вопросов и минимальное количество символов для ответа на каждый вопрос (Рисунок 22).

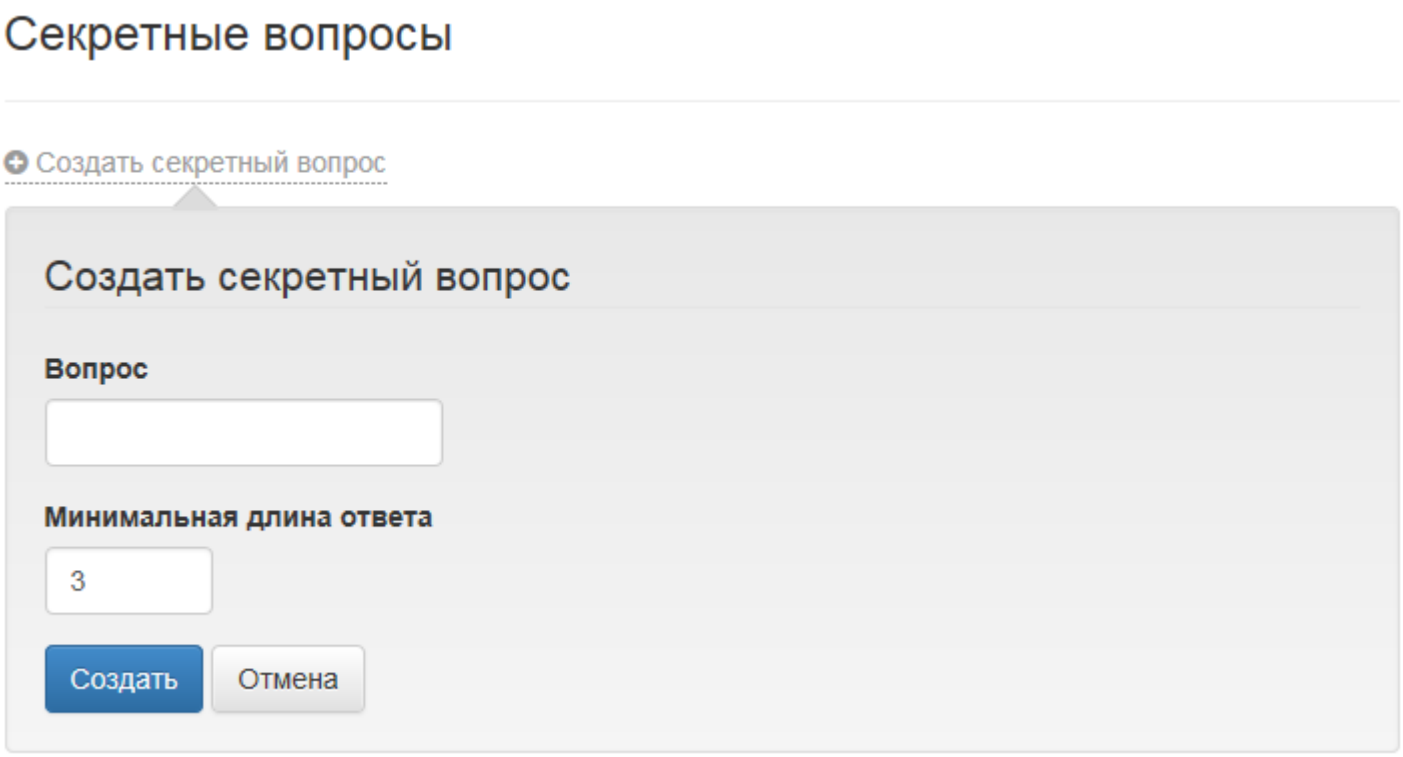

Рисунок 22 – Создание секретного вопроса.

Чтобы задать секретный вопрос, нажмите **Создать секретный вопрос**, введите вопрос и задайте минимальную длину ответа (значение по умолчанию – 3 символа). Нажмите кнопку **Создать** для сохранения параметров. Созданные вопросы в случае необходимости могут быть изменены или удалены. Чтобы изменить вопрос, нажмите ✎ напротив нужного вопроса. Для удаления вопроса нажмите ✖ (Рисунок 23).

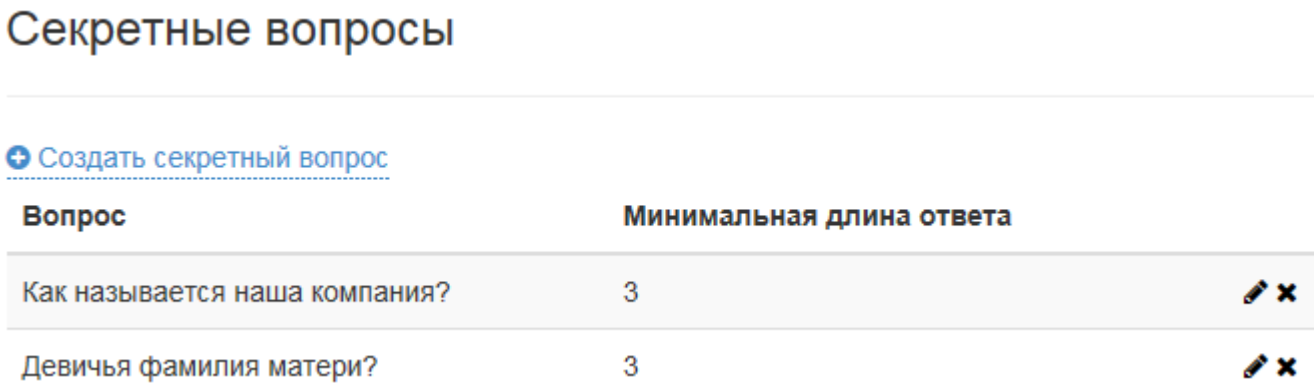

Рисунок 23 – Список созданных секретных вопросов.

Секретный вопрос может быть удален только в том случае, если его не использует ни один из пользователей системы.

Принтер смарт-карт. Интеграция Indeed CM с принтером EDIsecure XID 8300 позволяет выполнять следующие сценарии:

- выпускать смарт-карты пользователям используя считыватели принтера (контактный и бесконтактный) без печати
- выпускать смарт-карты пользователям используя считыватели принтера (контактный и бесконтактный) с печататью на карте изображения или текста
- печатать на смарт-картах изображение или текст без выпуска карты пользователям

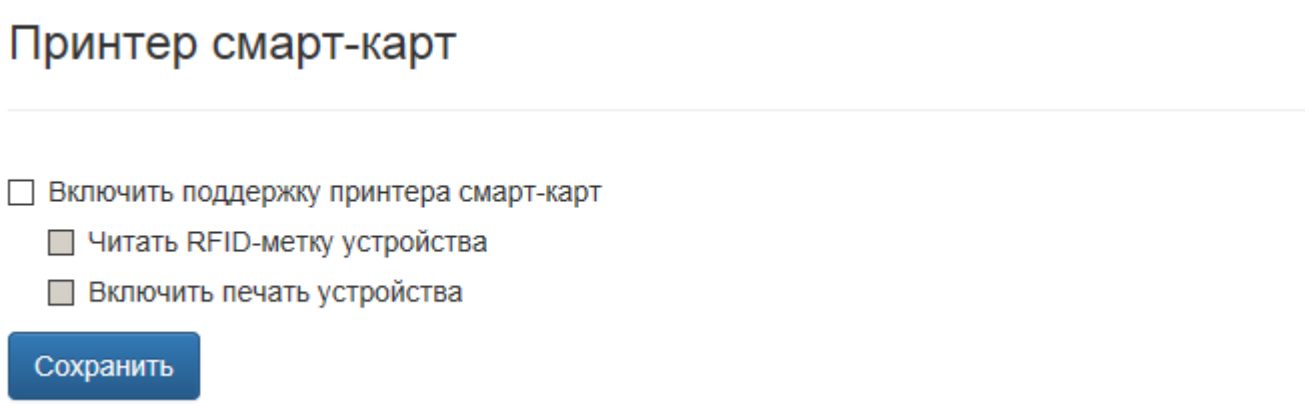

Рисунок 24 – Параметры работы с принтером смарт-карт.

Опция **Включить поддержку принтера смарт-карт** (Рисунок 24) позволяет при выпуске выбирать считыватель, к которому подключена карта: считыватель, подключенный к рабочей станции или считыватель принтера. При включении опции становятся доступны опции выпуска устройства с использованием принтера:

- **Читать RFID-метку устройства**
  Если опция включена, то Indeed CM прочитает метку устройства и сохранит её в свою базу данных связав с пользователем, для которого выпускается устройство. При отзыве устройства значение метки останется в хранилище Indeed CM до тех пор, пока устройство находится в системе. При выпуске устройства другому пользователю, значение метки закрепляется за ним.

- **Включить печать устройства**
  Если опция включена, то при выпуске устройства через принтер будет происходить печать изображения/теста на нем в соответствии с загруженным шаблоном печати.

На вкладке **Шаблон устройства** задается шаблон печати данных при выпуске смарт-карты в текущей политике. Шаблон представляет собой xml-файл, содержащий данные о том, что необходимо выводить на печать.

Для загрузки шаблона нажмите **Загрузить шаблон устройства**, укажите файл шаблона[13] и нажмите кнопку **Загрузить** (Рисунок 25). После загрузки шаблона его статус в политике ("не загружен") изменится на имя, указанное в файле шаблона.

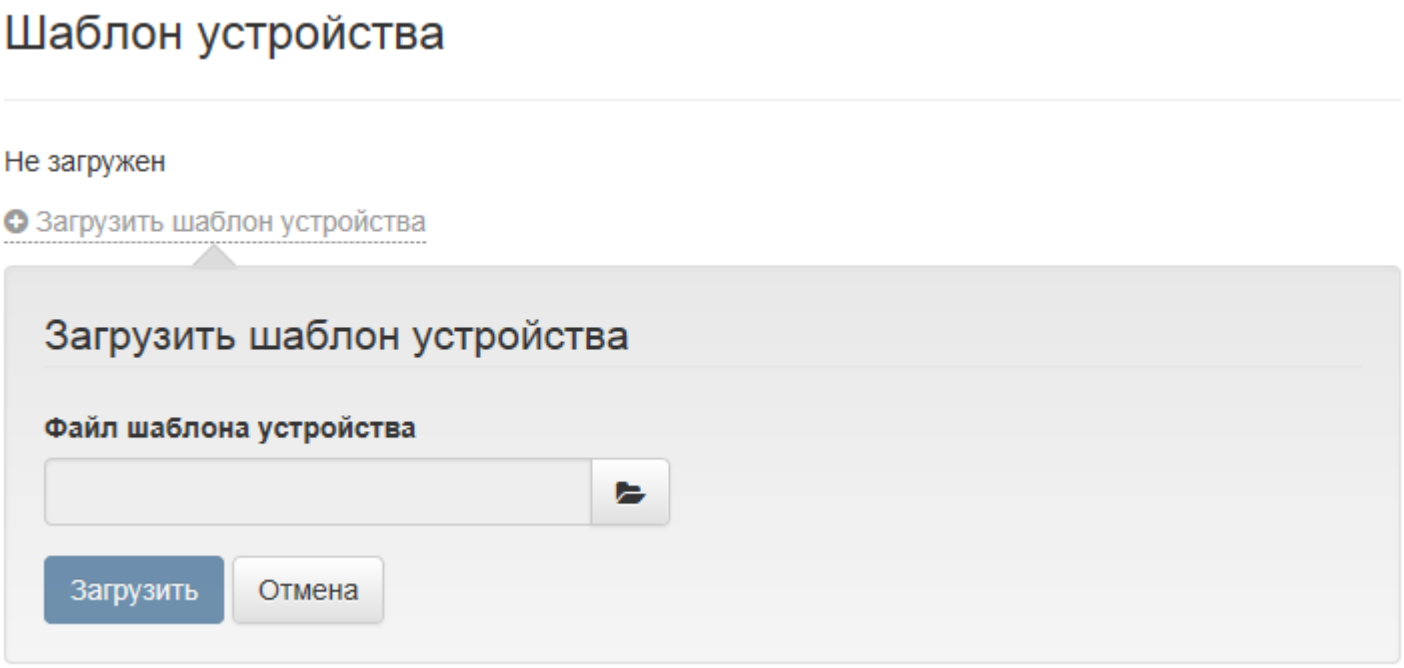

Рисунок 25 – Добавление шаблона печати.

Уведомления. В разделе задаются настройки почтовых уведомлений о событиях Indeed CM. Задайте настройки почтового сервера и определите получателей (администраторы или обычные пользователи). Пример настроек приведен на Рисунке 26.

[13]Файл шаблона печати можно получить обратившись в службу технической поддержки компании Индид.

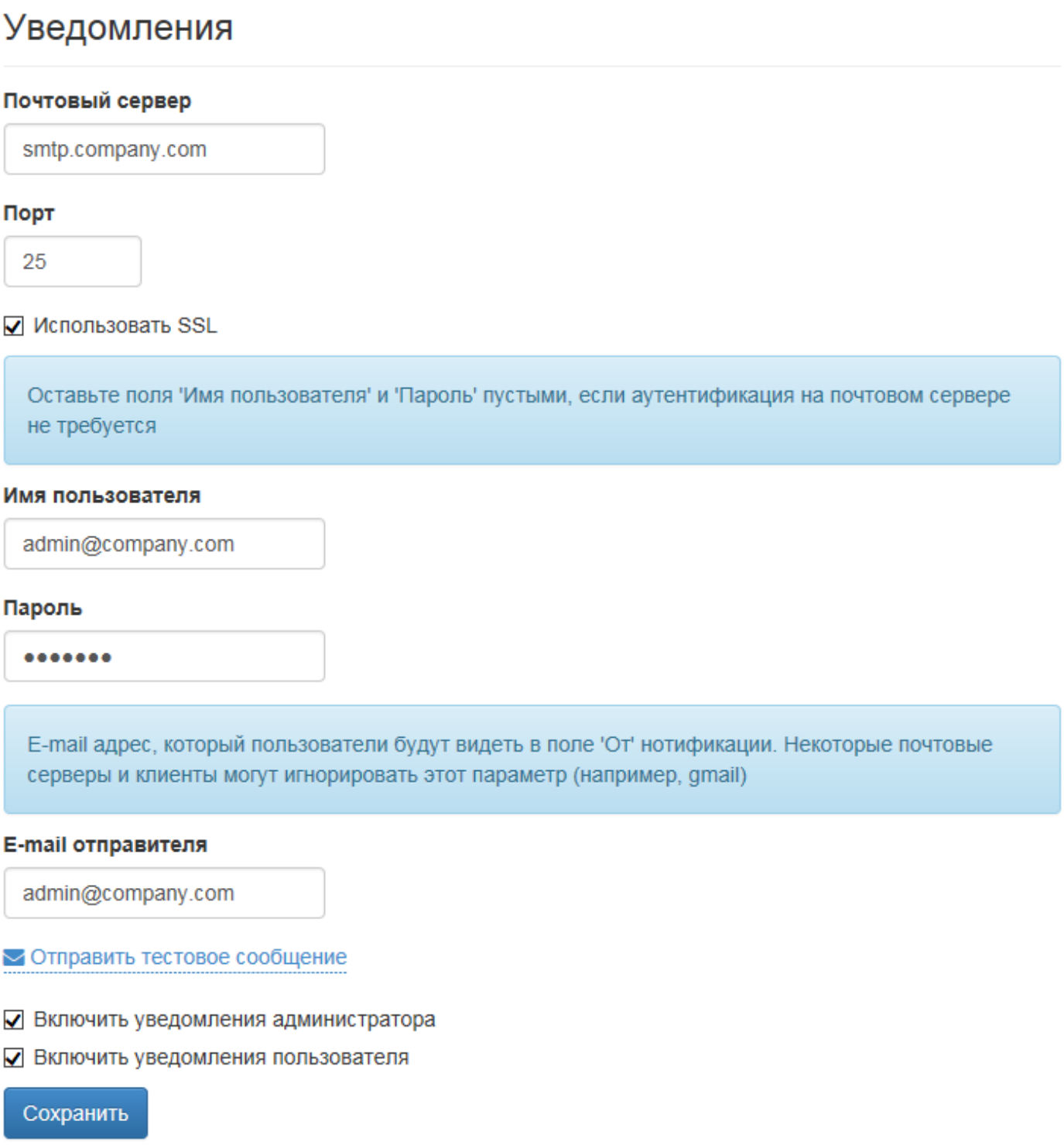

Рисунок 26 – Настройки уведомлений о событиях Indeed CM.

Воспользуйтесь функцией отправки тестового сообщения для проверки заданных настроек почтового сервера. Для этого укажите необходимые настройки почтового сервера, нажмите **Сохранить**, а затем **Отправить тестовое сообщение** (Рисунок 27).

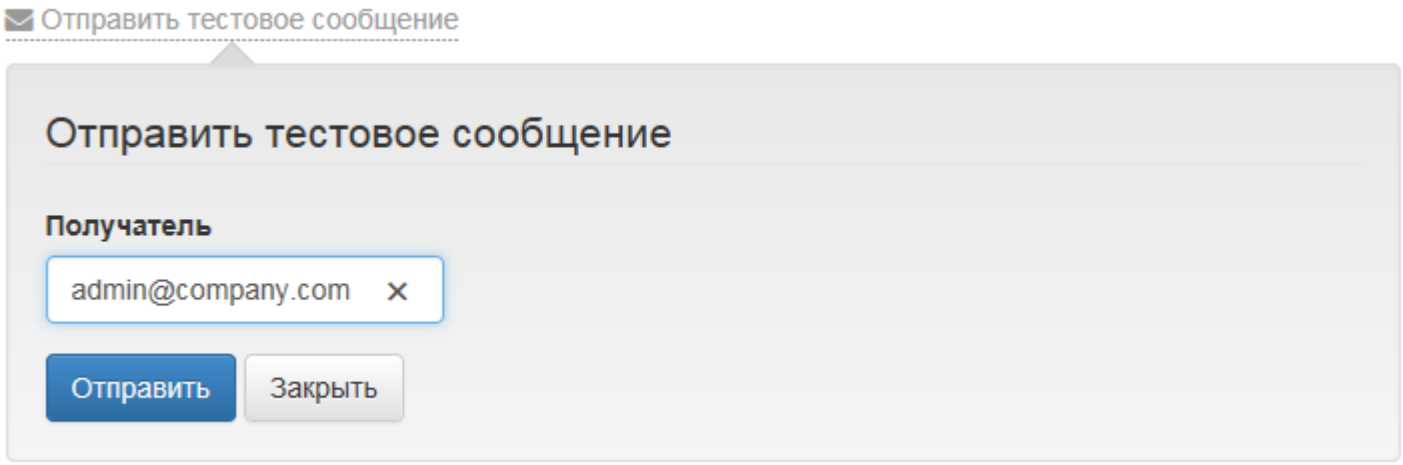

Рисунок 27 – Отправка тестового сообщения.

Укажите адрес электронной почты получателя и нажмите **Отправить**. Если настройки указаны верно, сообщение будет отправлено (Рисунок 28).

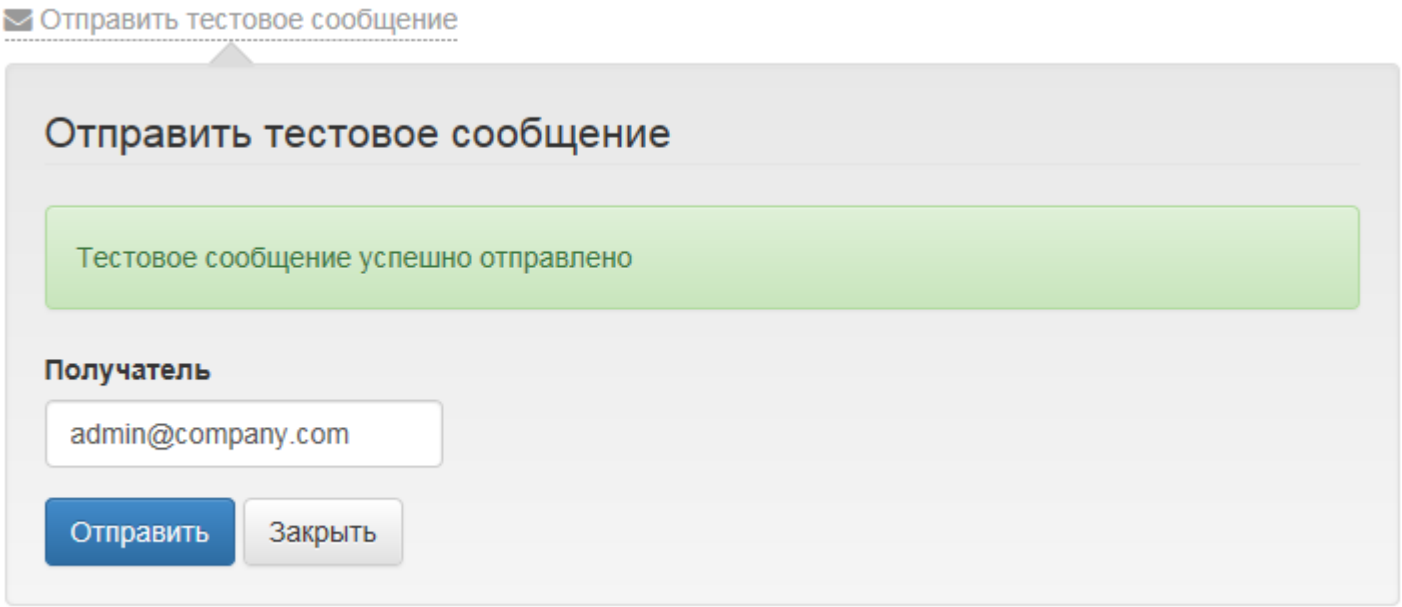

Рисунок 28 – Тестовое сообщение успешно отправлено.

Нажмите кнопку **Закрыть**. Если тестовое сообщение отправить не удалось, измените настройки почтового сервера, нажмите **Сохранить** и повторите попытку.

В пункте **Группы получателей** настраиваются группы получателей уведомлений администраторов. Например, это могут быть специалисты по информационной безопасности и защите информации вашей компании. Для того чтобы установить группу получателей нажмите **Создать группу**, укажите имя группы, введите адреса получателей и нажмите **Создать** (Рисунок 29).

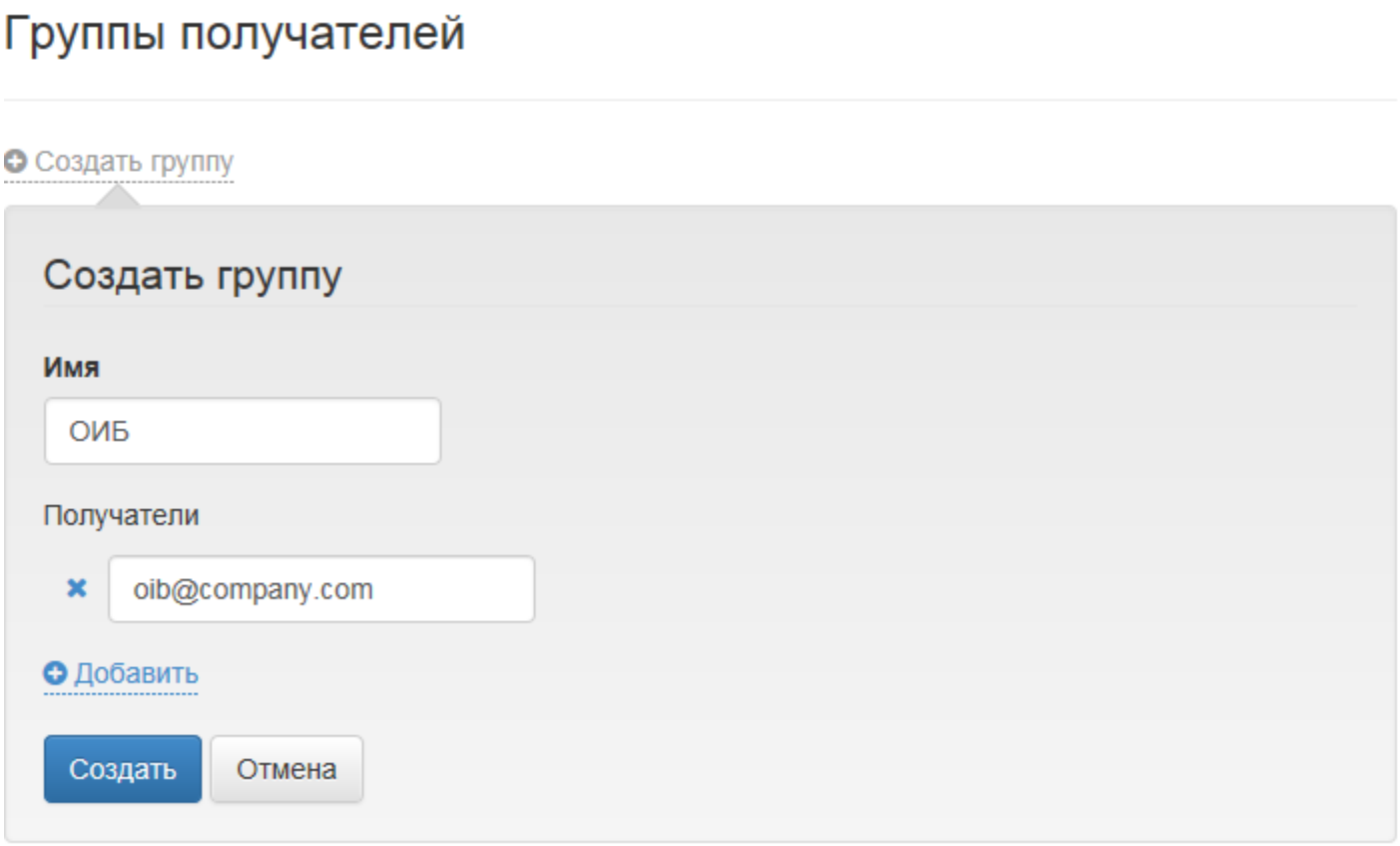

Рисунок 29 – Создание группы получателей.

Созданные группы получателей в случае необходимости могут быть изменены или удалены (Рисунок 30). Для изменения группы выберите ее в списке и нажмите ✎. Для удаления группы нажмите ✖.

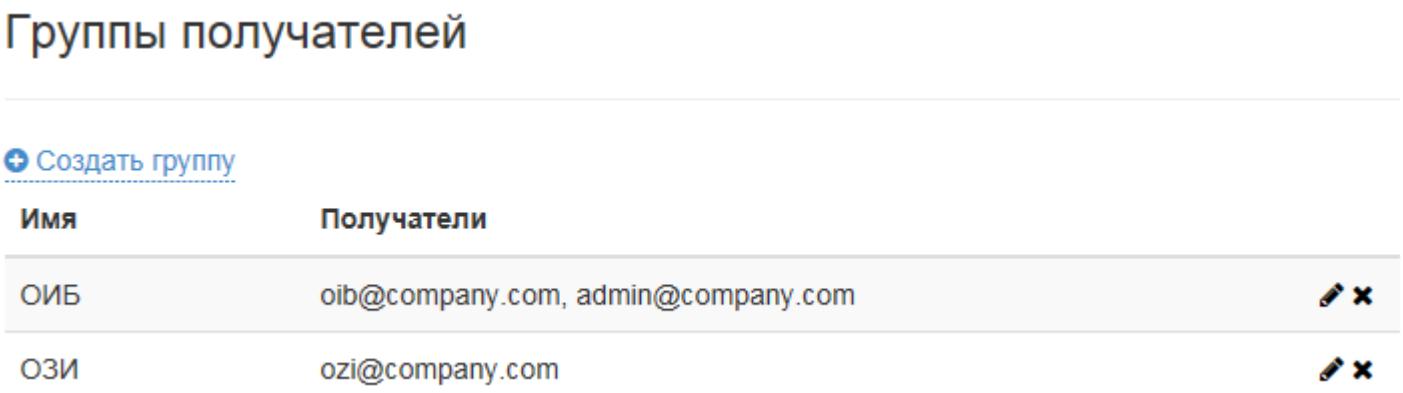

Рисунок 30 – Список групп получателей.

Группа получателей может быть удалена только в том случае, если она не используется для рассылки уведомлений.

В пункте **Уведомления администратора** необходимо выбрать событие системы, тип события и группу получателей.
Система может быть настроена для оповещения о следующих событиях:

- Назначение устройства
- Отвязка устройства
- Выпуск устройства
- Выпуск сертификата
- Включение устройства
- Выключение устройства
- Отзыв устройства
- Обновление устройства
- Замена устройства
- Очистка устройства
- Сброс PIN-кода
- Разблокировка устройства
- Изменение PIN-кода
- Выпуск устройства ожидает решения
- Обновление карте ожидает решения
- Замена устройства ожидает решения
- Отмена обновления устройства
- Одобрение выпуска устройства
- Отклонение выпуска устройства
- Одобрение обновления устройства
- Отклонение обновления устройства
- Одобрение замены устройства
- Отклонение замены устройства
- Содержимое устройства истекает
- Отслеживаемые сертификаты истекают
- Политика была обновлена
- Политика пользователя была изменена
- Изменение ответов на секретные вопросы
- Аутентификация
- Блокировка пользователя
- Разблокировка пользователя
- Сброс ответов на секретные вопросы
- Изменение политики
- Добавление СКЗИ
- Обновление СКЗИ

- Уничтожение/изъятие СКЗИ
- Добавление AirKey к компьютеру
- Создание кода подключения AirKey к компьютеру
- Удаление AirKey от компьютера
- Выпуск сертификата

Система может быть настроена для оповещения о следующих типах событий:

- Информация
- Ошибка
- Предупреждение

В качестве адресатов могут быть выбраны:

- Приложение - группа созданная в разделе **Группы получателей**
- Каталог пользователей - группа безопасности Active Directory

Для создания уведомления нажмите **Создать уведомление**, выберите событие и укажите тип события, о котором необходимо извещать администратора (Информация, Ошибка или Предупреждение), укажите группу получателей и нажмите **Создать** (Рисунок 31).

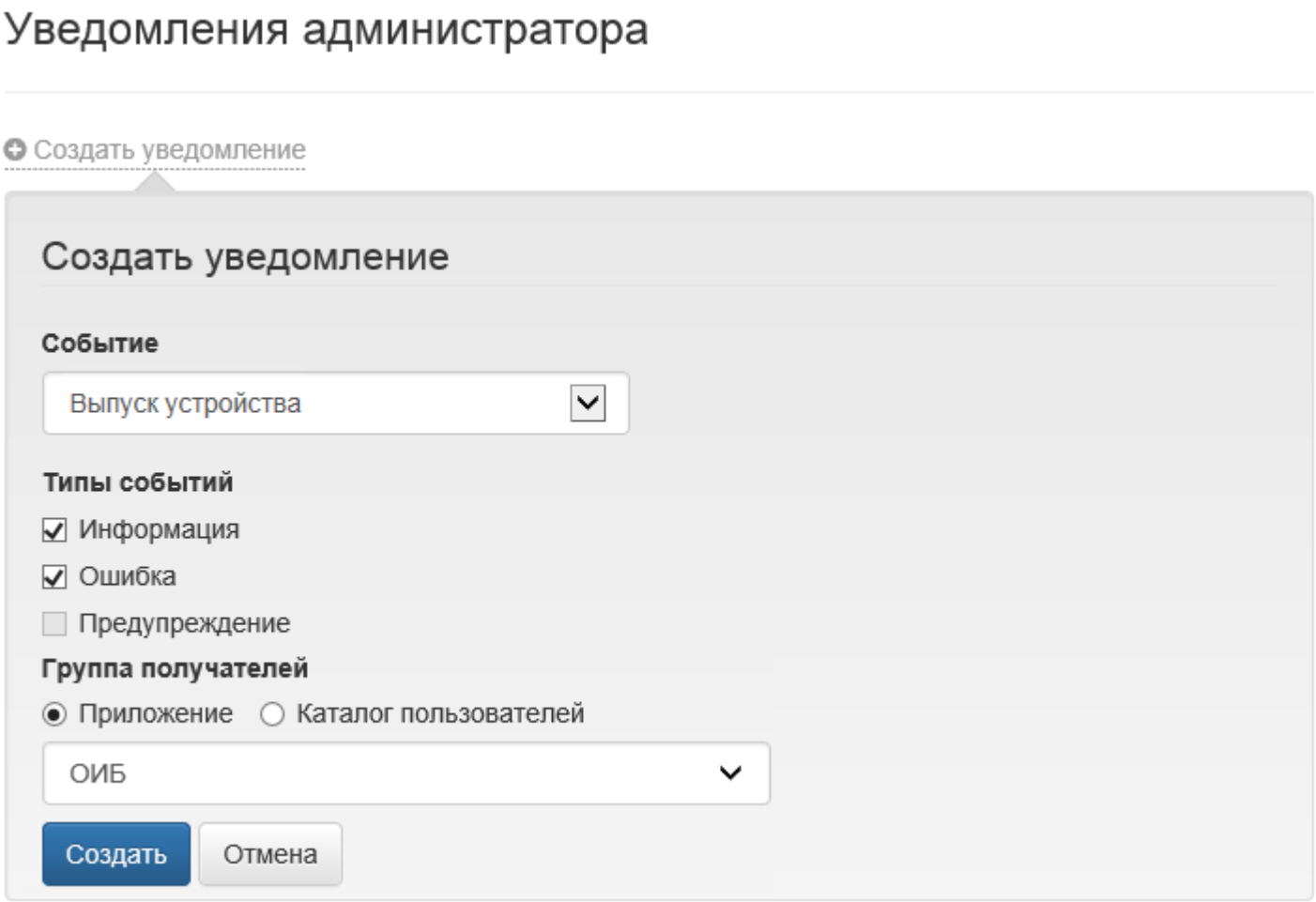

Рисунок 31 – Создание уведомления администратора.

Созданные уведомления в случае необходимости могут быть изменены или удалены. Для изменения уведомления выберите его в списке и нажмите ✎. Для удаления уведомления нажмите ✖ (Рисунок 32).

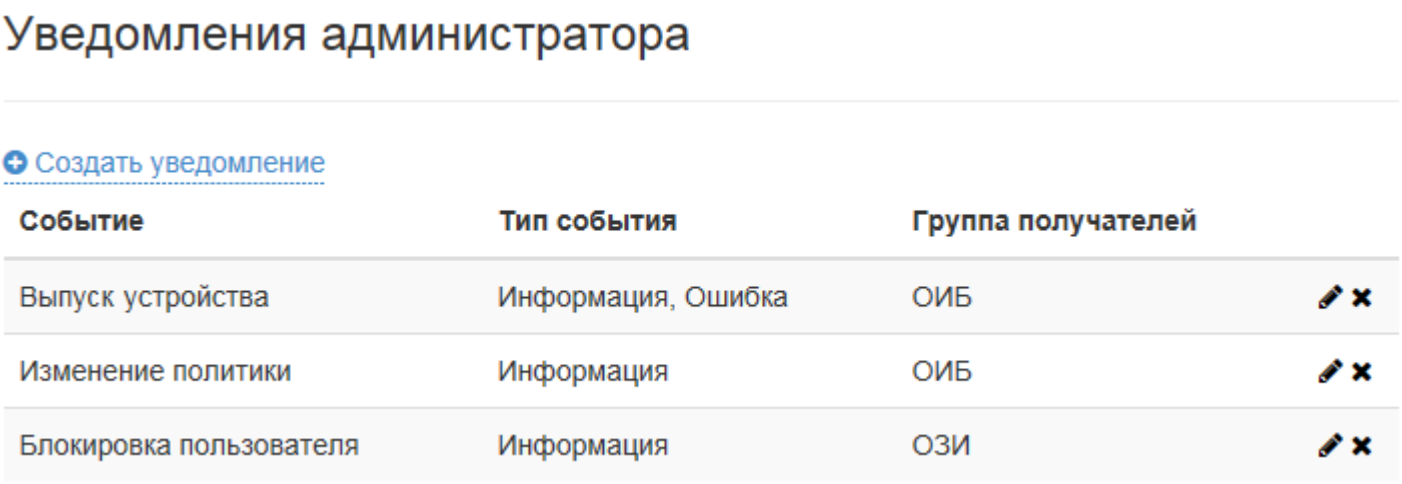

Рисунок 32 – Список созданных уведомлений администратора.

В пункте **Уведомления пользователя** настраивается перечень событий системы, о которых необходимо извещать пользователей. Система может быть настроена для оповещения о следующих событиях:

- Назначение устройства
- Отвязка устройства
- Выпуск устройства
- Выпуск сертификата
- Включение устройства
- Выключение устройства
- Отзыв устройства
- Обновление устройства
- Замена устройства
- Очистка устройства
- Сброс PIN-кода
- Разблокировка устройства
- Изменение PIN-кода
- Выпуск устройства ожидает решения
- Обновление устройства ожидает решения
- Замена устройства ожидает решения
- Отмена обновления устройства
- Одобрение выпуска устройства
- Отклонение выпуска устройства
- Одобрение обновления устройства
- Отклонение обновления устройства

- Одобрение замены устройства
- Отклонение замены устройства
- Содержимое устройства истекает
- Отслеживаемые сертификаты истекают
- Политика была обновлена
- Политика пользователя была изменена
- Установка PIN-кода
- Изменение ответов на секретные вопросы
- Аутентификация
- Блокировка пользователя
- Разблокировка пользователя
- Сброс ответов на секретные вопросы
- Добавление AirKey к компьютеру
- Создание кода подключения AirKey к компьютеру
- Удаление AirKey от компьютера
- Добавление СКЗИ
- Обновление СКЗИ
- Уничтожение/изъятие СКЗИ
- Выпуск сертификата

Для создания уведомления нажмите **Создать уведомление**, выберите событие, о котором необходимо извещать пользователя и укажите тип (Рисунок 33).

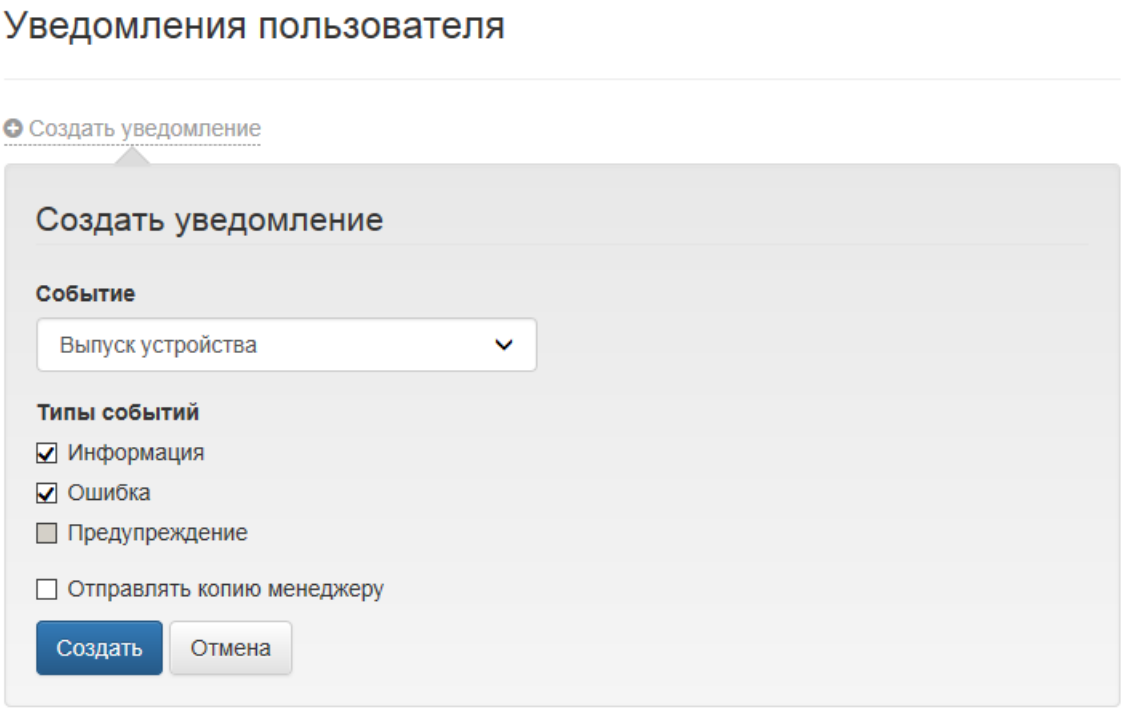

Рисунок 33 – Создание уведомления пользователя.

Уведомления о событиях системы отправляются только тем пользователям, у которых в свойствах учетной записи Active Directory указан адрес электронной почты. Адрес электронной почты руководителя (менеджера) задается в профиле соответствующего пользователя Active Directory. Имя руководителя (менеджера) задается на вкладке **Организация** (Organization) свойств пользователя Active Directory в разделе **Руководитель** (Manager).

Если необходимо, включите опцию отправки сообщения о выбранном событии руководителю (менеджеру) пользователя[14] и нажмите **Создать**.
Для изменения уведомления выберите его в списке и нажмите ✎. Для удаления уведомления нажмите ✖.
В пункте **Шаблоны администратора** настраиваются шаблоны почтовых уведомлений о событиях системы, которые будут рассылаться администраторам Indeed CM. В базовом варианте почтовое уведомление содержит следующую информацию:

Тема. Формируется исходя из названия события, например, «Выпуск устройства».

Текст сообщения. Формируется исходя из названия сообщения и его типа, может содержать информацию об инициаторе, пользователе, сертификатах и устройствах (Рисунок 34).

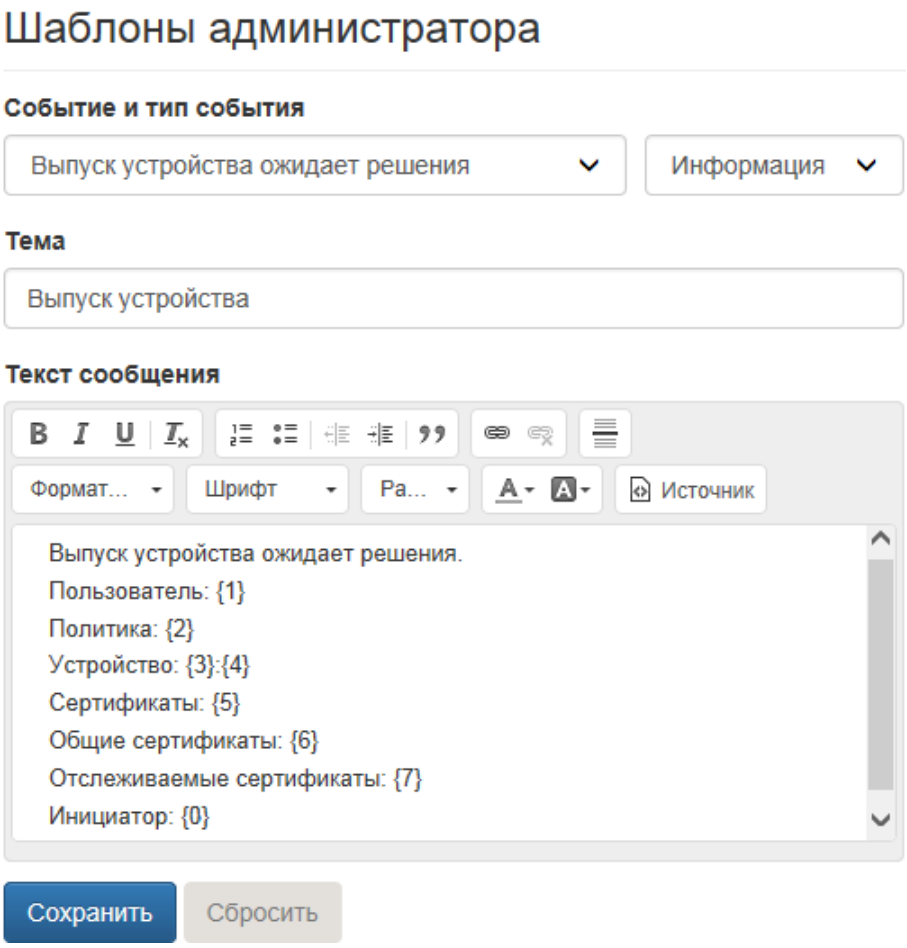

Рисунок 34 – Базовый шаблон почтового уведомления администратора системы.

[14]Только для пользователей, расположенных в Active Directory.

Для каждого уведомления в одной политике использования устройств настраивается только один шаблон. На основе базового шаблона, представленного на Рисунке 34, Indeed CM сформирует и отправит электронное письмо следующего содержания:

```
Тема: Выпуск устройства
Текст сообщения: Выпуск устройства ожидает решения.
Политика: MSCA+КриптоПро 2.0
Устройство: Rutoken S:0755398982
Сертификаты: Квалифицированный пользователь, Пользователь
Общие сертификаты: Сертификат для VPN
Отслеживаемые сертификаты: Пользователь VIPNet
Инициатор: DEMO\Administrator
```

Базовый шаблон может быть изменен. Система позволяет использовать HTML-теги для форматирования текста сообщения. На Рисунке 35 приведен пример персонализированного шаблона почтового уведомления.

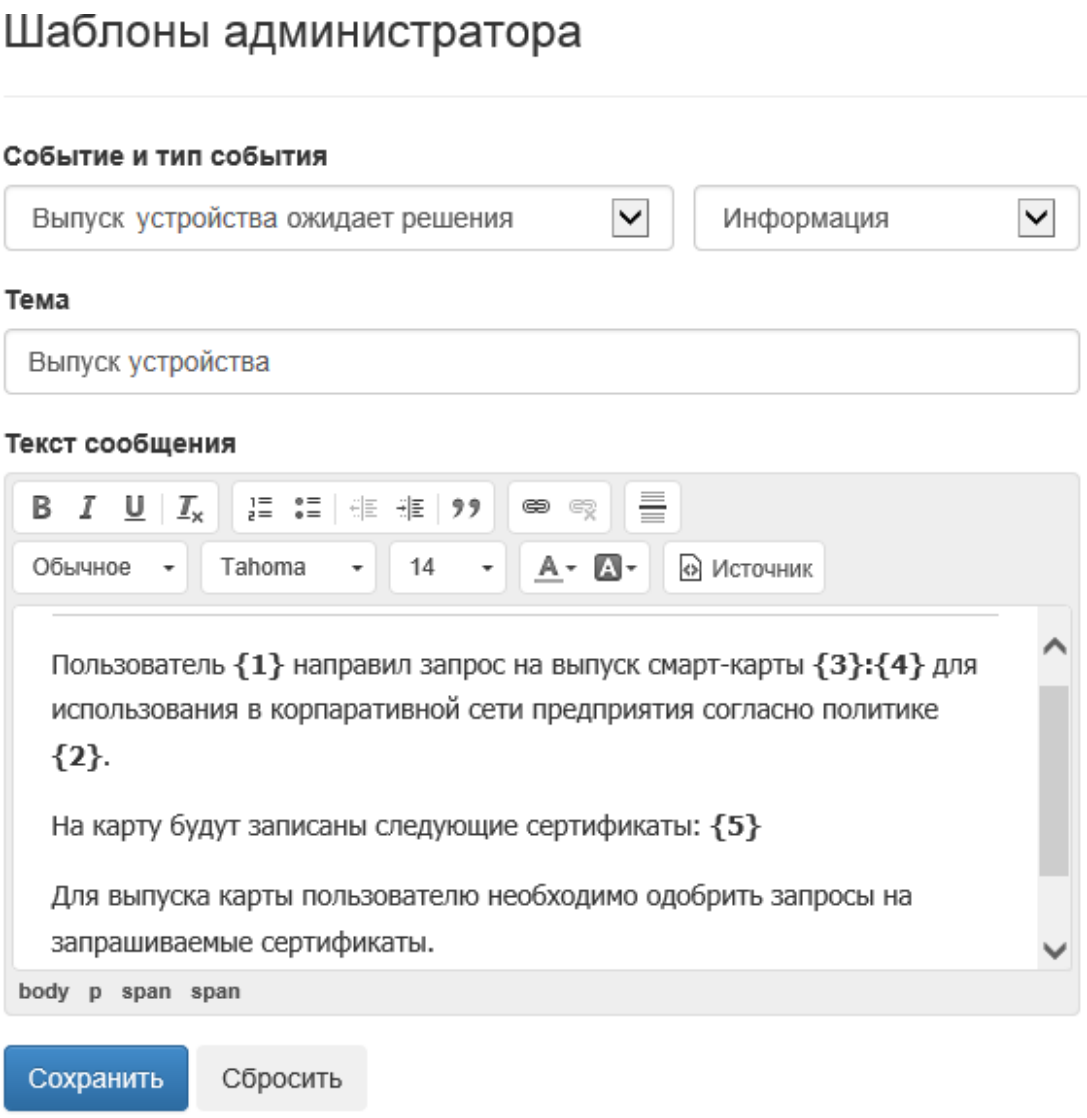

Рисунок 35 – Измененный шаблон почтового уведомления администратора системы.

Текст почтового уведомления, созданного на основе изменённого базового шаблона, будет таким:
Тема: Выпуск устройства пользователя ожидает решения

Пользователь **Евгений Белов** направил запрос на выпуск смарт-карты **Rutoken S:0756309531**, для использования в корпоративной сети предприятия согласно политике **Базовая политика**.
На карту будут записаны следующие сертификаты: **Квалифицированный пользователь, Пользователь Удостоверяющего Центра**.
Для выпуска устройства пользователю необходимо одобрить запросы на запрашиваемые сертификаты.

В пункте **Шаблоны пользователя** настраиваются шаблоны почтовых уведомлений о событиях Indeed CM, которые будут рассылаться пользователям. Для каждого уведомления в одной политике использования устройств настраивается один шаблон. В базовом варианте почтовое уведомление содержит следующую информацию:

Тема. Формируется исходя из названия события, например, «Выпуск устройства».

Текст сообщения. Формируется исходя из названия сообщения и его типа, может содержать информацию об инициаторе, пользователе и устройствах.

Базовый шаблон может быть изменен в зависимости политики безопасности, используемой в вашей компании. Например, текст письма может быть дополнен сообщением о конфиденциальности, содержащейся в нем информации, либо дополнен указаниями к действиям, которые должны предпринять сотрудники, получившее письмо.
Нажмите **Сохранить** для сохранения] политики. Для удаления политики выберите её в списке и нажмите **×** . Подтвердите действие нажатием кнопки **Удалить**.

Политику можно удалить только в том случае, если она не используется (т.е. в Indeed CM нет ни одного устройства, выпущенного с применением этой политики).

Назначения политик

Политики использования устройств начнут действовать на пользователей после определения области действия. Политика может распространяться на следующие объекты:

Active Directory:

- Домен (Domain)
- Контейнер (Container)
- Подразделение (Organizational Unit)

Действие политики может распространяться как на весь объект (домен, контейнер или подразделение), так и на отдельные группы пользователей, входящие в него.

КриптоПро УЦ 2.0:

- Часть существующей в Центре Регистрации структуры контейнеров (папок) или на весь ЦР

Организационная структура Indeed CM, в узлы которой могут входить:

- Домен (Domain), контейнер (Container), подразделение (Organization Unit), пользователи или группы безопасности Active Directory
- Часть существующей в Центре Регистрации структуры контейнеров (папок) или на весь ЦР. Пользователи или группы безопасности ЦР.

Политики, действующие на каталог пользователей Active Directory или каталог Центра Регистрации КриптоПро УЦ 2.0 имеют приоритет над политиками, действующими на Организационную структуру Indeed CM.

Для назначения политики на объект нажмите **Создать назначение политики**, выберете политику из списка и задайте следующие параметры (Рисунок 36):

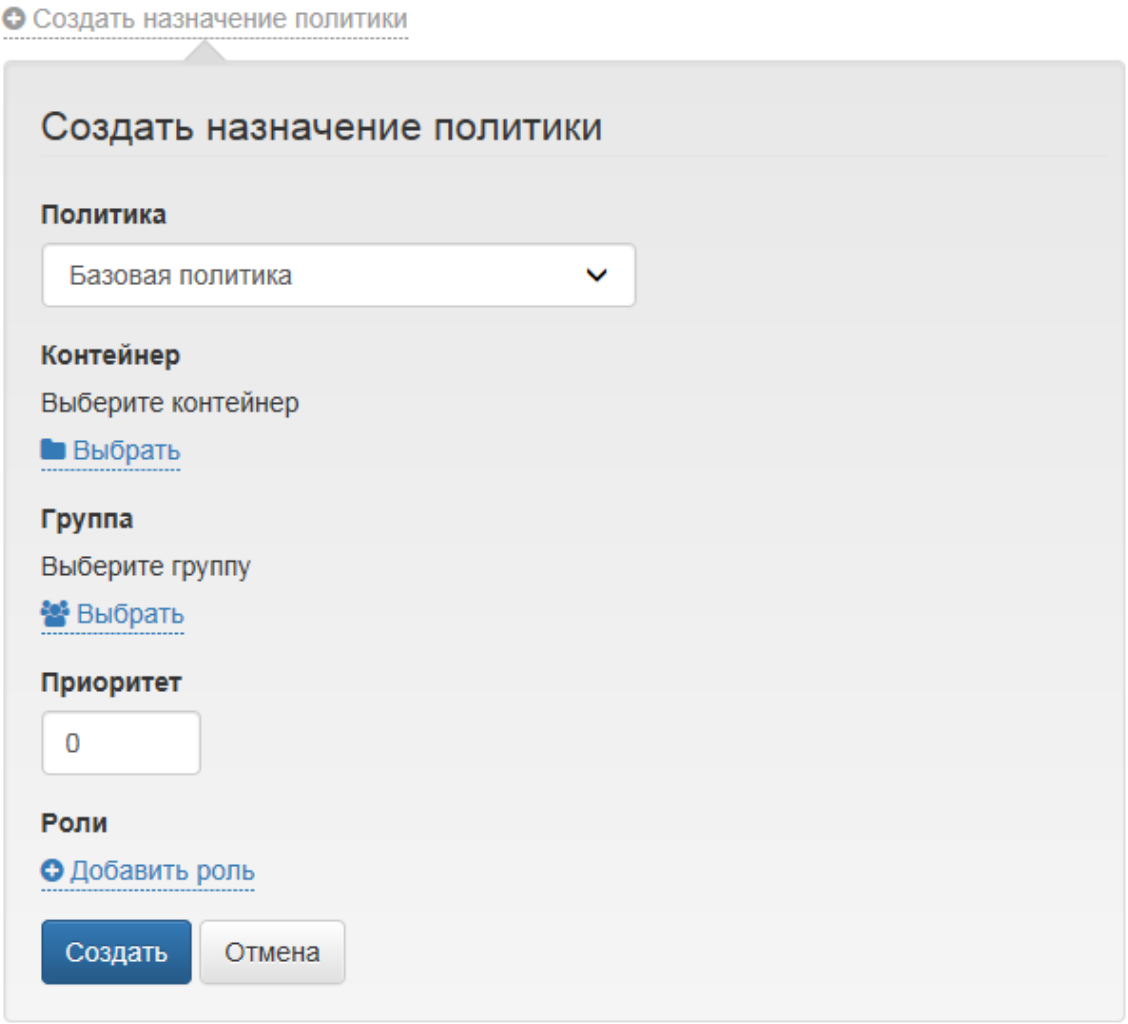

Рисунок 36 – Назначение политики.

- **Контейнер и группа** – область действия политики. Контейнером может быть подразделение Active Directory, папка Центра Регистрации КриптоПро УЦ 2.0 или узел организационной структуры Indeed CM.
  Группа – дополнительный фильтр для распространения политики. Например, на один контейнер с пользователями организации может быть назначено несколько политик, которые будут распространяться на пользователей, входящих в определенные группы Active Directory.
- **Приоритет** – значение, определяющее применение той или иной политики к пользователю. Если пользователь попадает под область действия нескольких политик выпуска устройств одного типа (политики Active Directory, ЦР КриптоПро УЦ или Организационной структуры), например, состоит в двух группах, расположенных в одном OU, то действовать на пользователя будет политика с бóльшим приоритетом.
- **Роли** – если в разделе Роли есть хотябы одна локальная роль, то ее можно будет добавить в создаваемое назначение политики и задать пользователей роли.

Нажмите **Создать** для сохранения назначения политики. Для изменения назначения политики нажмите ✎. Для удаления назначения нажмите ✖ (Рисунок 37):

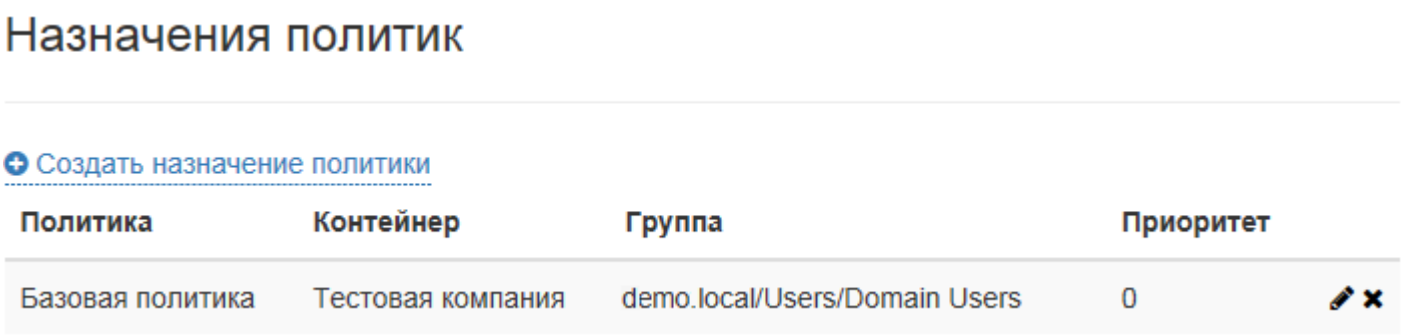

Рисунок 37 – Назначения политик.

Роли

Полномочия пользователей в Indeed CM настраиваются в разделе **Роли**. Роли могут быть глобальными (распространяться на все политики использования устройств) и локальными (распространяться только на указанные политики). Добавление локальных ролей в политики осуществляется в разделе Назначения политик. Предустановленными являются глобальные роли **Администраторов** и **Операторов** (Рисунок 38).

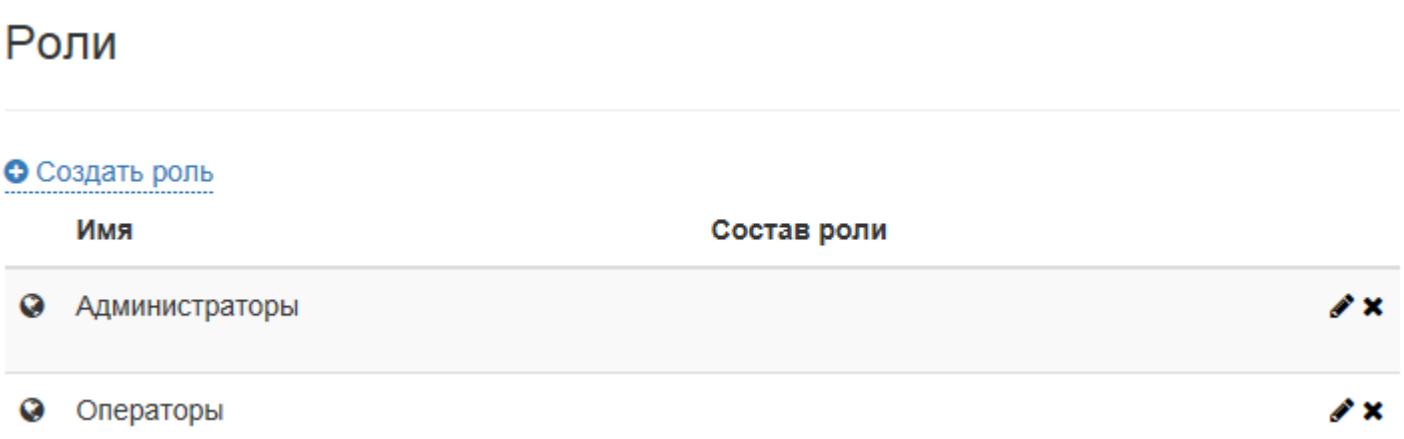

Рисунок 38 – Предустановленные глобальные роли Indeed CM.

Для членов роли задается набор разрешенных и запрещенных действий. По умолчанию предустановленная роль администраторов имеет максимальные полномочия, а операторы ограничены в правах на конфигурирование системы. Для изменения роли нажмите . Пользователи включаются в состав роли персонально или через членство в группах Active Directory.
Состав глобальных ролей формируется при их создании или редактировании. Состав локальных ролей задается при добавлении роли в политику в разделе Назначения политик.
Для добавления пользователя в глобальную роль нажмите **Добавить** и найдите пользователя или группу в каталоге (Рисунок 39):

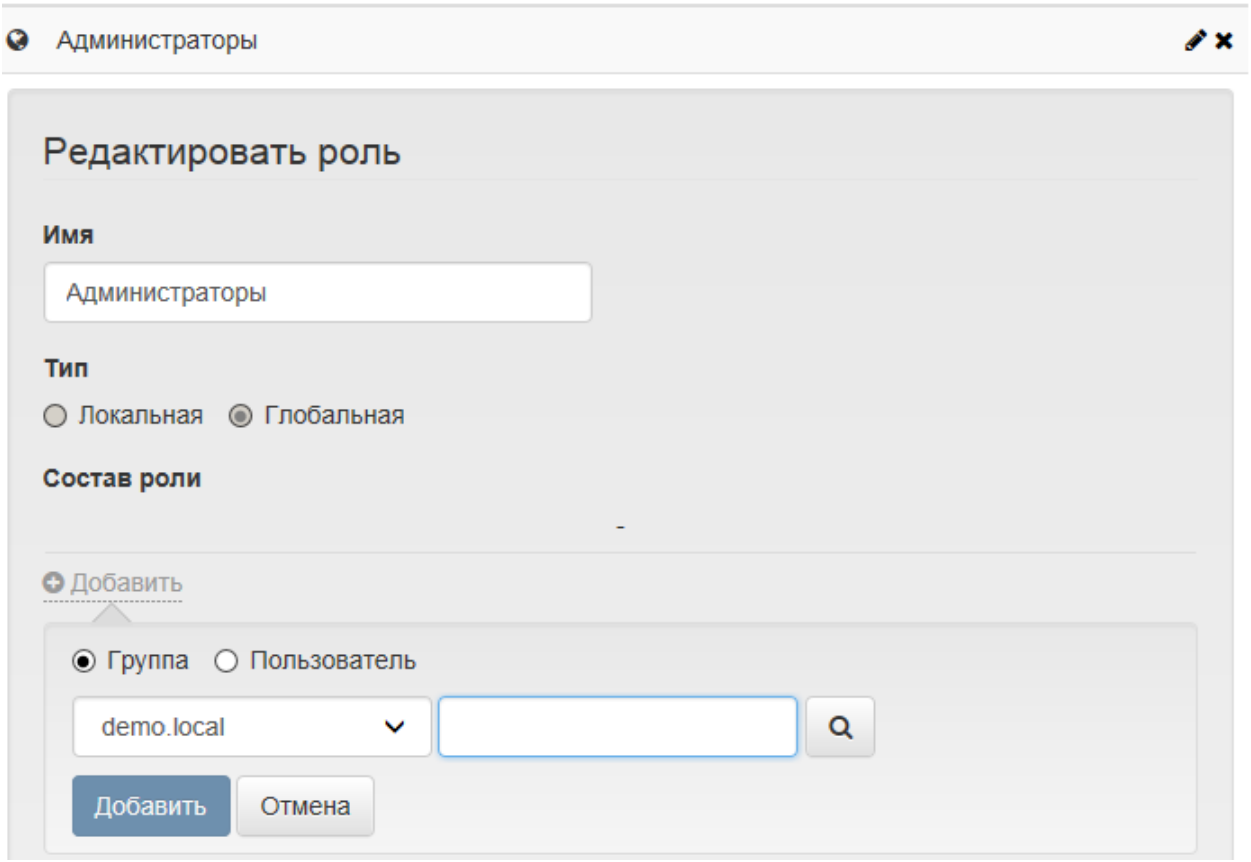

Рисунок 39 – Добавление группы пользователей в роль.

Задайте привилегии для членов роли (Рисунок 40):

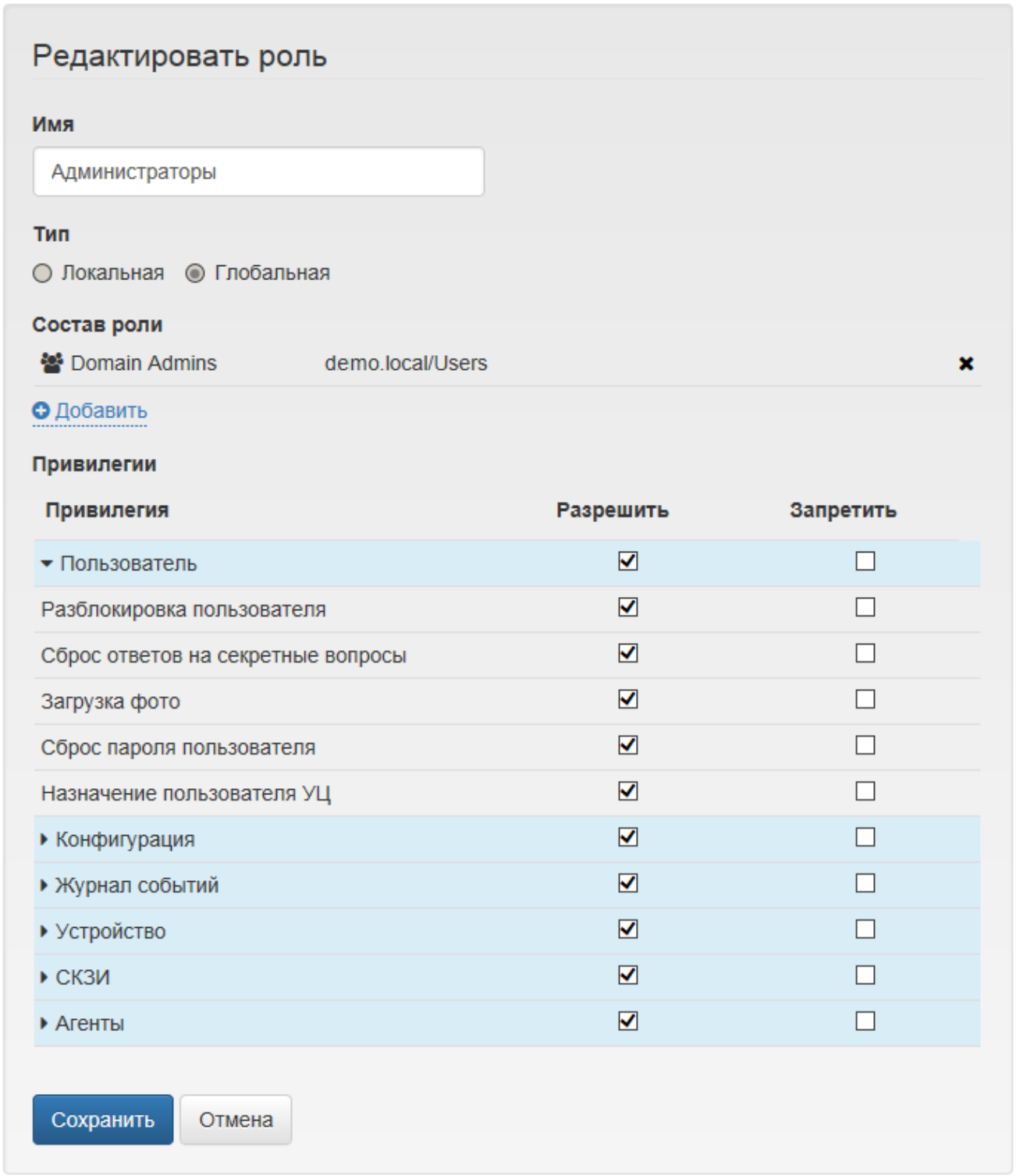

Рисунок 40 – Настройка привилегий для членов роли.

Нажмите **Сохранить** для применения внесенных изменений. Тип роли (глобальная или локальная) нельзя изменить после создания роли. Состав и набор привелегий доступны для изменения при редактировании роли.

Работа в Indeed CM

Устройства

Раздел для поиска устройств в Indeed CM и добавления новых.

Добавление устройства

Добавьте устройство в Indeed CM для начала работы. При добавлении устройства PIN-код администратора, заменяется на случайный или указанный в разделе **Конфигурация – Типы устройств**.

После добавления устройства с установкой случайного PIN-кода администратора вне Indeed CM будет невозможно разблокировать PIN-код пользователя и провести инициализацию отдельных видов устройств.

При удалении устройства из Indeed CM PIN-код администратора заменяется на указанный в файле типа устройства. Для добавления устройства нажмите **Добавить устройство** (Рисунок 41).

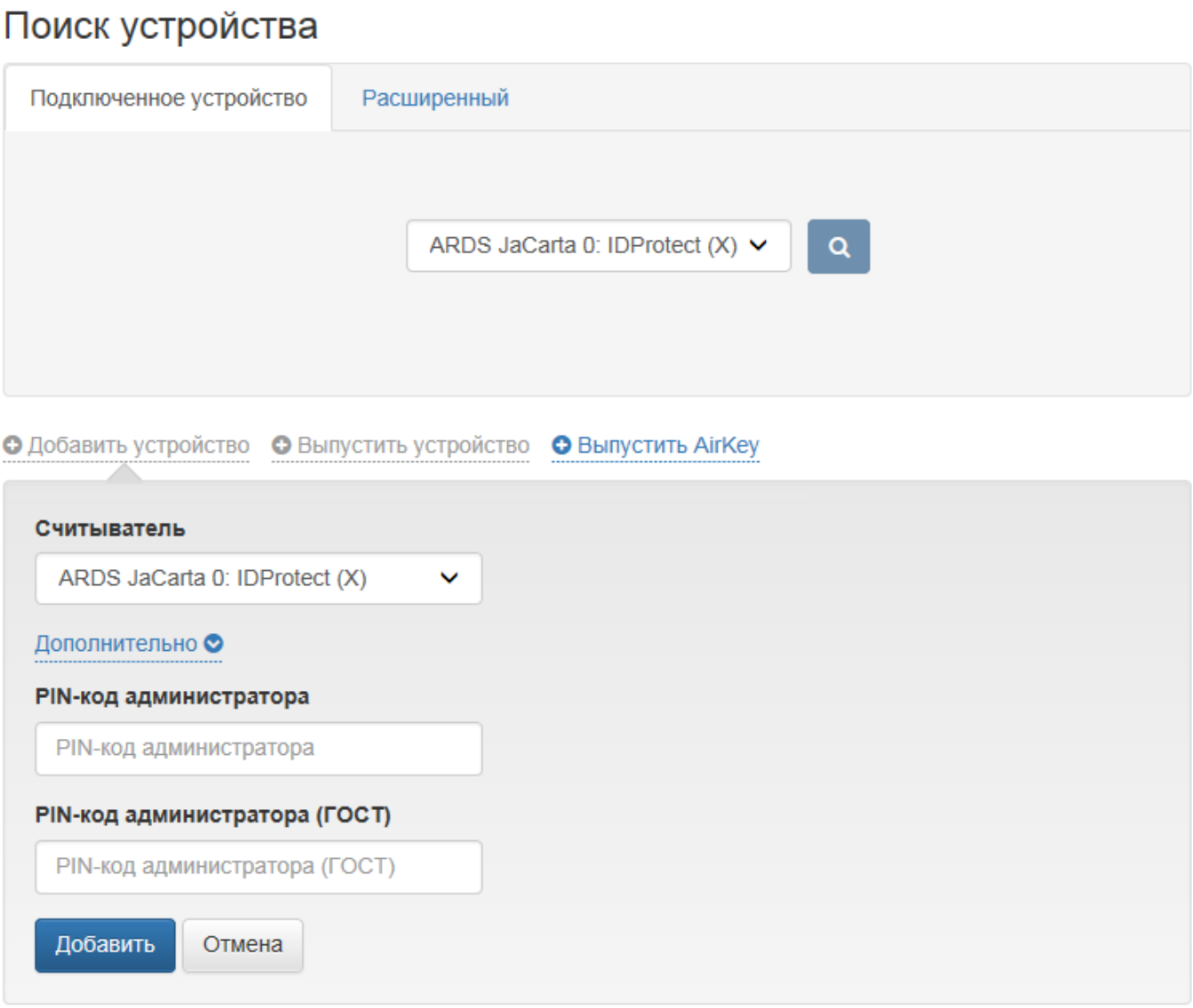

Рисунок 41 – Добавление устройства.

Устройство добавляется двумя способами:

- **Без указания PIN-кода администратора** – установленный на устройстве PIN-код администратора должен совпадать с указанным в разделе **Конфигурация – Типы устройств**.
- **С указанием PIN-кода администратора** – установленный на устройстве PIN-код администратора указывается в одноименном поле после нажатия кнопки **Дополнительно** (Рисунок 41).

Подключите устройство к компьютеру, задайте PIN-код администратора (если это необходимо) и нажмите **Добавить**. После добавления устройства нажмите **Закрыть** (Рисунок 42). Устройства можно добавлять автоматически подключая их последовательно к одному и тому же считывателю.

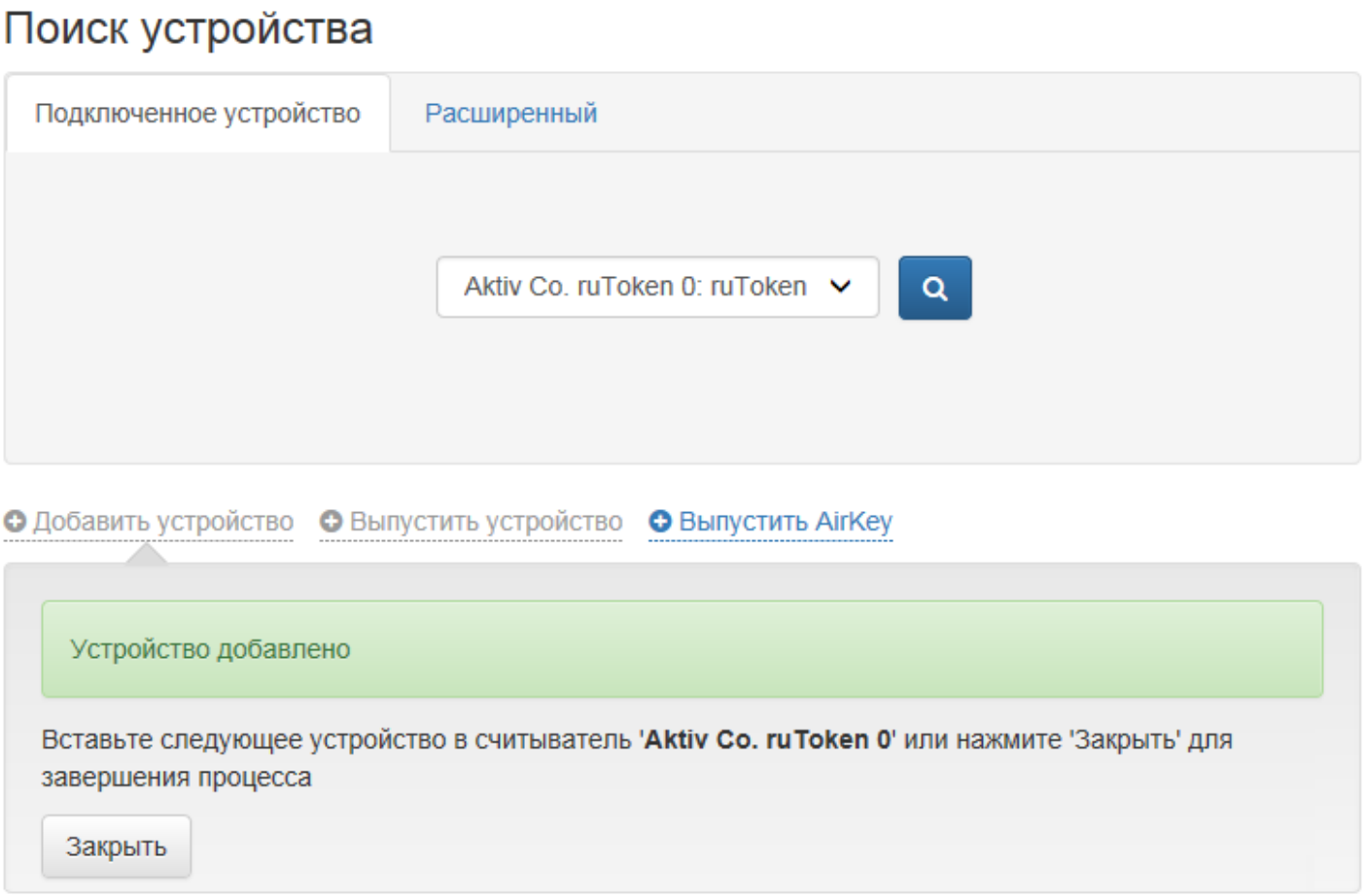

Рисунок 42 – Устройство успешно добавлено.

Поиск устройства

Поиск устройств происходит двумя способами: поиск по подключенному устройству и расширенный поиск по нескольким параметрам.

Поиск по подключенному устройству применяется в случае, если устройство физически доступно, но никаких других данных о нем нет (например, сотрудник нашел утерянный usb-токен и передал его администратору).

Перейдите на вкладку **Подключенное устройство**, подключите устройство к компьютеру и нажмите  (Рисунок 43).

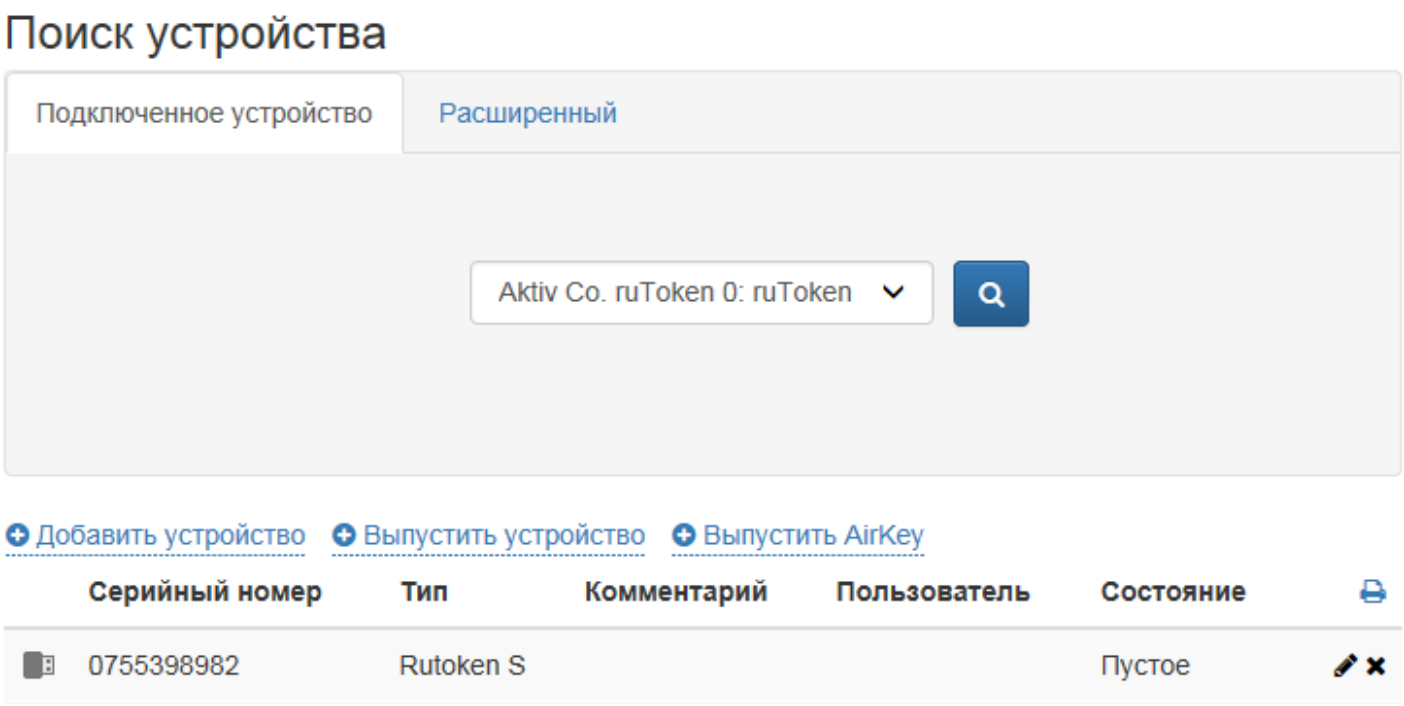

Рисунок 43 – Поиск по подключенному устройству.

Расширенный поиск применяется в случае, если устройство физически недоступно, но известны некоторые его данные (серийный номер или его часть, тип, комментарий, статус содержимого, имя пользователя, состояние). Поиск осуществляется по одному или нескольким (всем) параметрам. Чтобы выполнить поиск, укажите известные данные устройства и нажмите (Рисунок 44).

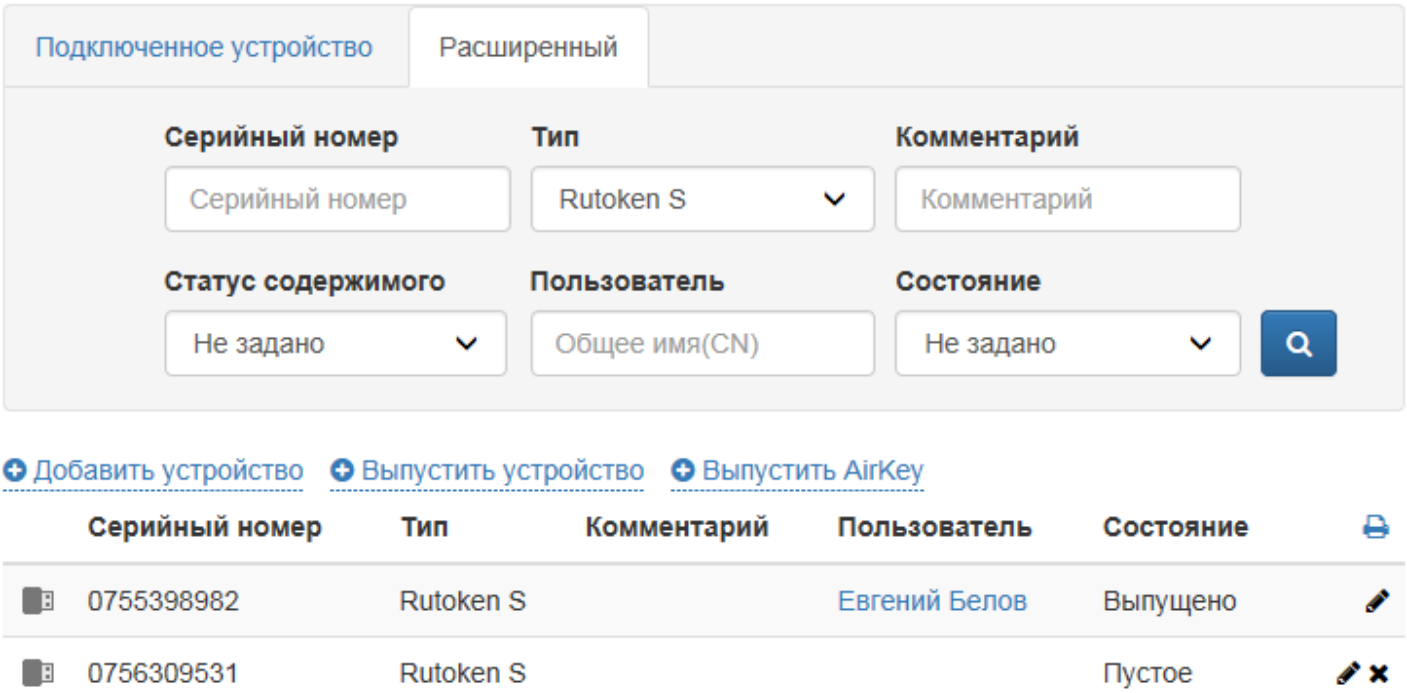

Рисунок 44 – Поиск устройства по его типу.

Для фильтрации карт по статусу содержимого требуется настроенный по расписанию запуск приложения Card Monitor.

Для вывода списка всех устройств введите символ ***** в поле **Серийный номер** и выполните поиск (Рисунок 45).

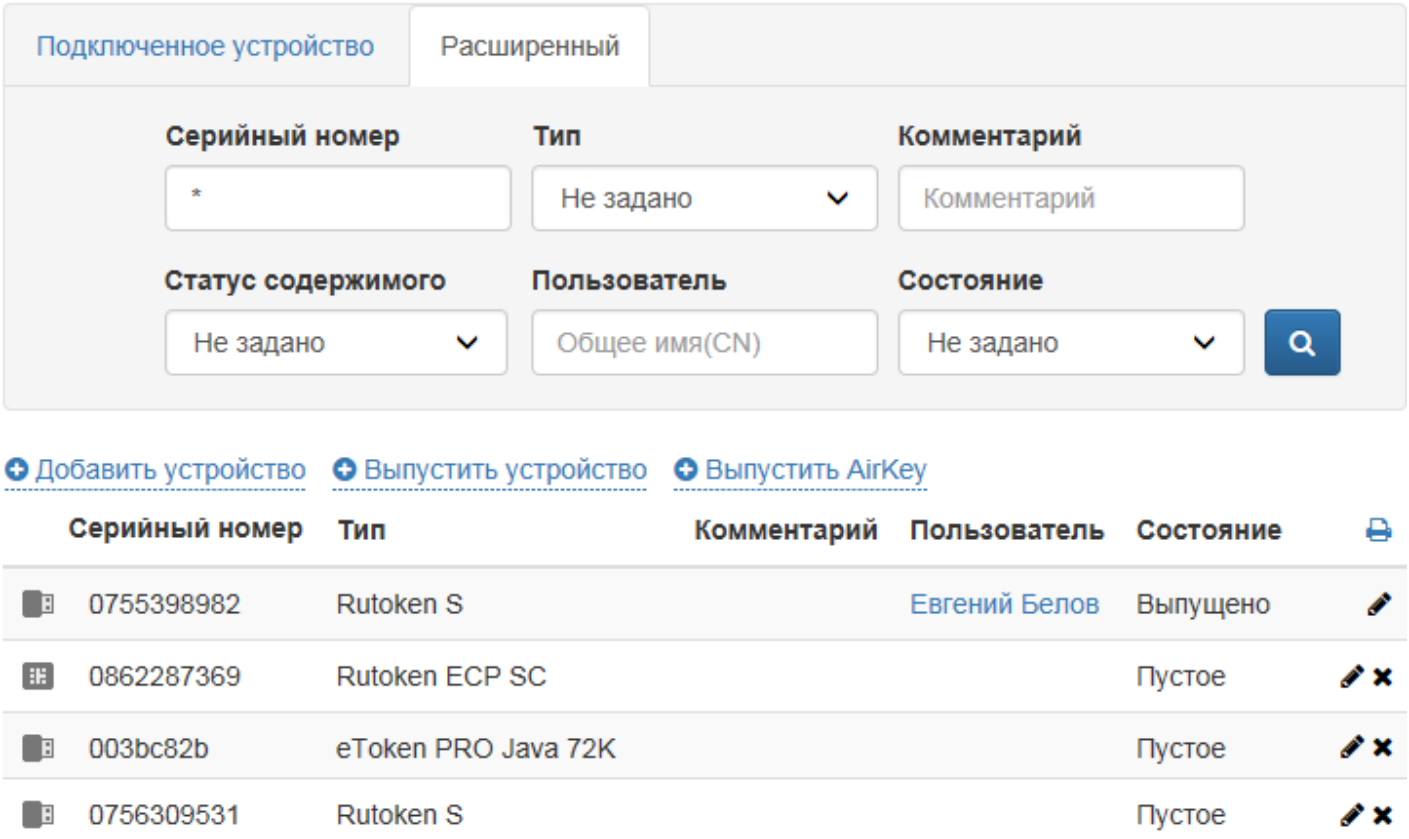

Рисунок 45 – Все устройства, зарегистрированные в системе.

Для поиска устройства по части серийного номера введите символ * и известную последовательность цифр в поле **Серийный номер**, выполните поиск (Рисунок 46).

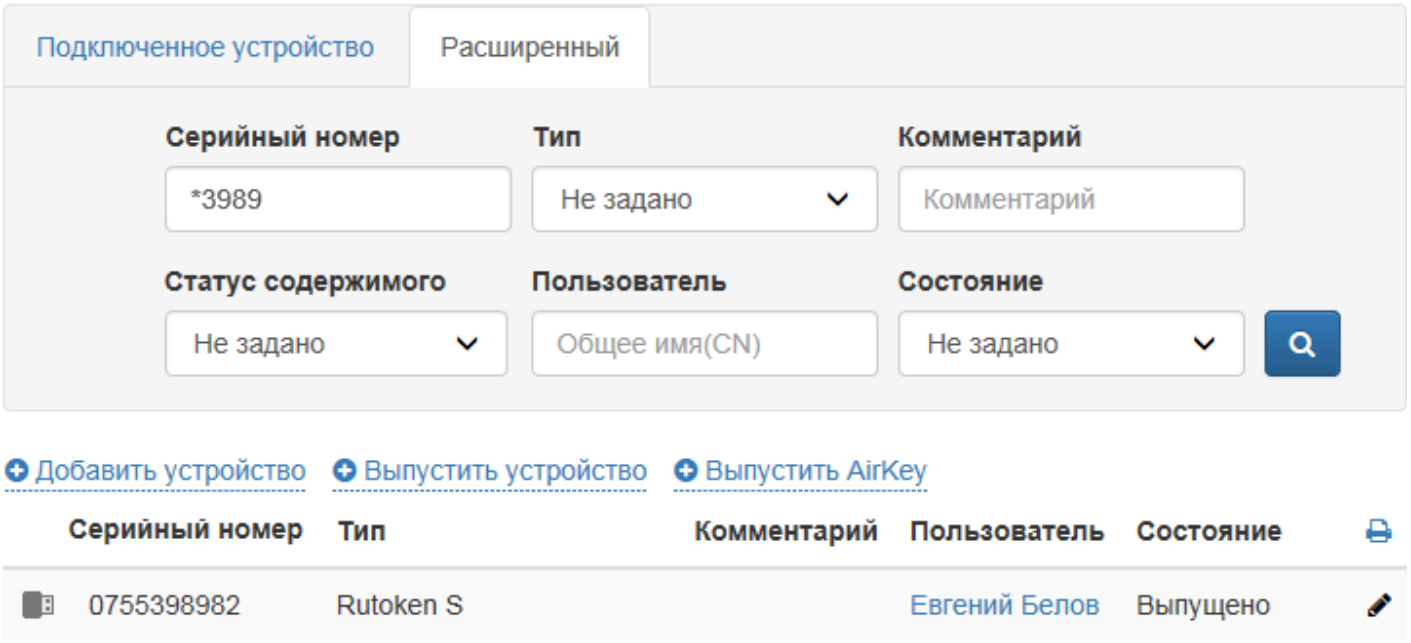

Рисунок 46 – Поиск по части серийного номера.

Для просмотра содержимого устройства нажмите ✎. Для просмотра PIN-кода администратора нажмите 👁 (Рисунок 47).

> Администраторам Indeed CM доступен просмотр PIN-кодов всех добавленных в систему устройств. Администраторам отдельных политик доступен просмотр только PIN-кодов устройств, назначенных/выпущенных пользователям этих политик.

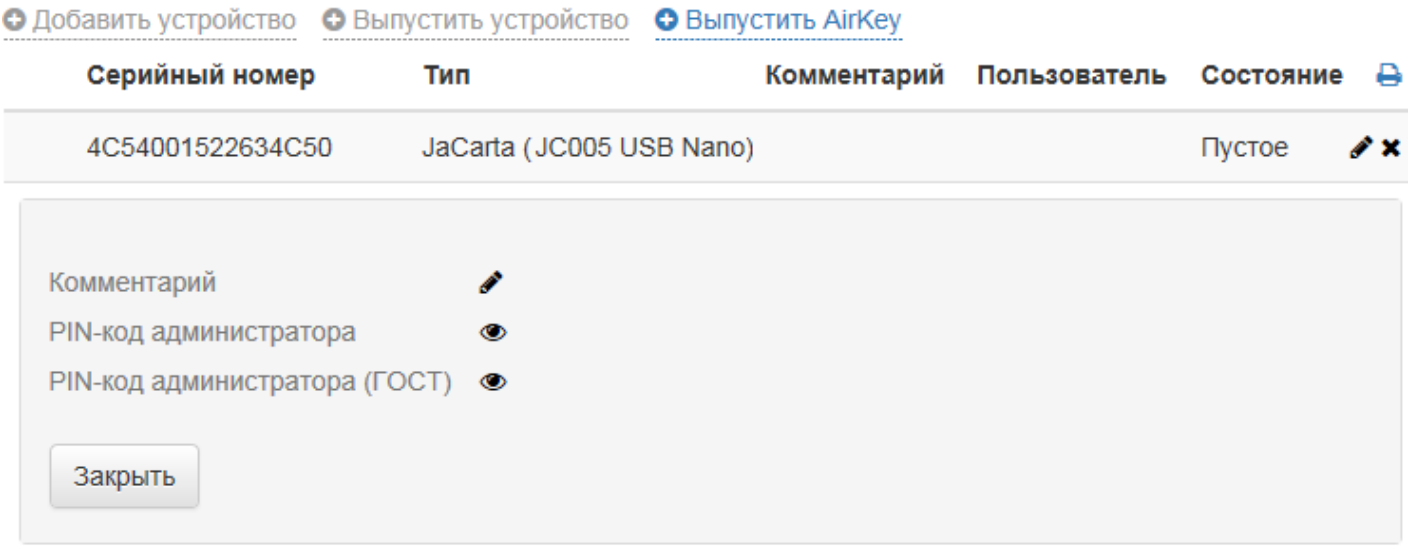

Рисунок 47 – Просмотр содержимого устройства.

Результаты поиска устройств могут быть сохранены в виде файла. Для создания файла с результатами поиска нажмите и выберите формат. Сохраните полученный файл.

Выпуск устройства

Выпуск устройств и виртуальных карт AirKey в разделе **Устройства** аналогичен выпуску из Карточки пользователя.

Удаление устройства

Удаление устройства из системы возможно как при наличии устройства, так и без него.

> Если PIN-код администратора устройства был изменен на случайный при добавлении устройства (опция **Устанавливать неслучайный PIN-код администратора** выключена в разделе **Конфигурация – Типы устройств**), то при удалении устройства без подключения к рабочей станции PIN-код администратора останется случайным и неизвестным!

Для удаления устройства выполните его поиск и нажмите ✖ (Рисунок 48).

Если устройство доступно, подключите его к компьютеру и нажмите **Удалить** (Рисунок 48).

> При включении опции **Инициализировать устройство** все содержимое (в том числе, сертификаты, записанные до ввода устройства в Indeed CM) будет удалено.

Если устройство недоступно, выберите соответствующий пункт и нажмите **Удалить**. Возможно изъятие устройства у пользователя, если оно было выпущено ранее и затем отозвано, без удаления из системы. Действие применимо как для доступного, так и для недоступного устройства.

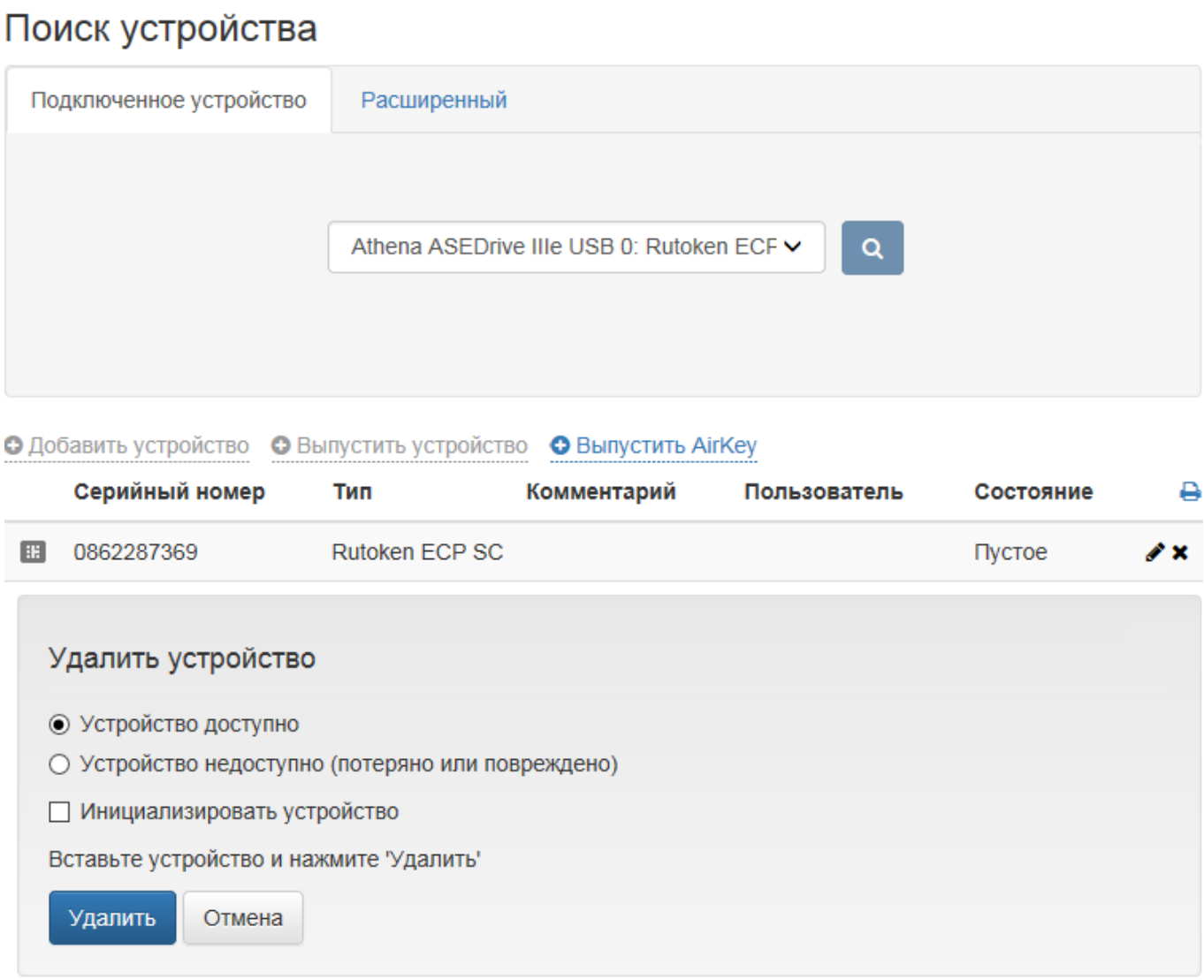

Рисунок 48 – Удаление устройства.

Пользователи

Раздел позволяет выполнять поиск пользователей и осуществлять для них следующие операции:

- Назначение устройства
- Выпуск устройства (в т.ч. виртуальной карты AirKey)
- Загрузка фотографии
- Сброс ответов на секретные вопросы
- Разблокировка пользователя
- Установка связи с пользователями Центра Регистрации КриптоПро УЦ 2.0
- Печать данных на устройстве
- Сброс PIN-кода
- Просмотр PIN-кода администратора устройства
- Изменение комментария устройства
- Разблокировка устройства

- Выключение и включение устройства
- Отзыв устройства
- Замена устройства
- Обновление устройства
- Добавление СКЗИ
- Редактирование СКЗИ
- Уничтожение СКЗИ
- Добавление компьютера к карте AirKey
- Удаление компьютера от карты AirKey

Для каждого пользователя возможен просмотр списка последних событий в Indeed CM. Раздел **Пользователи** открывается автоматически при переходе на страницу приложения Management Console.

Поиск пользователя

Для выполнения действия с устройством, имеющего отношение к пользователю системы, необходимо выполнить поиск нужного пользователя среди всех пользователей каталога. Существует два варианта поиска пользователей: простой и расширенный.

Простой поиск пользователя выполняется по заданным в строке символам: sAMAccountName, Common name, имени, фамилии и адресу электронной почты. Введите символ ***** в строке поиска для просмотра пользователей каталога. Результаты поиска выводятся после нажатия кнопки  или клавиши **Enter** в виде таблицы с полями: Общее имя(CN), Имя и фамилия, E-mail, Контейнер, Устройства (Рисунок 49).

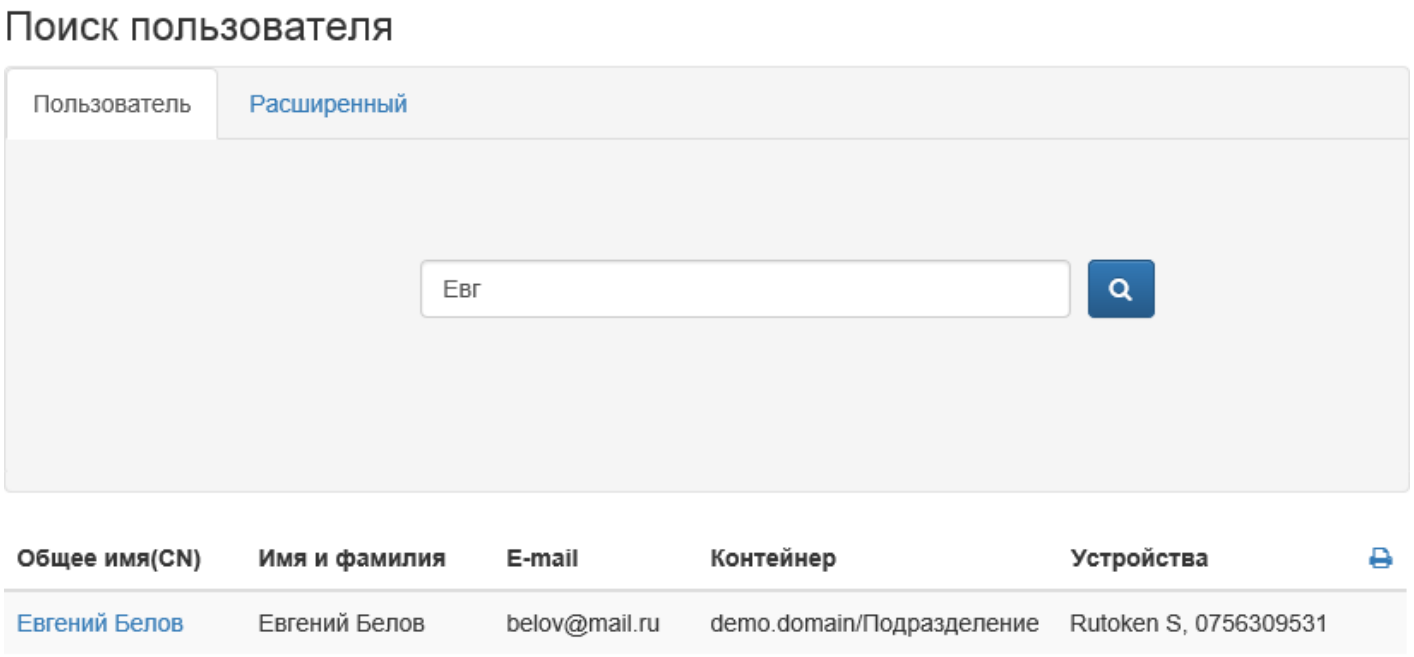

Рисунок 49 – Простой поиск пользователя.

Расширенный поиск может выполняться по нескольким параметрам: Common Name, имени, фамилии и контейнеру (Рисунок 50). Поиск может осуществляться как по одному параметру (например, фамилии) так и по нескольким (например, все пользователи с фамилией, начинающейся на “Б”, находящиеся в указанном контейнере или подразделении).

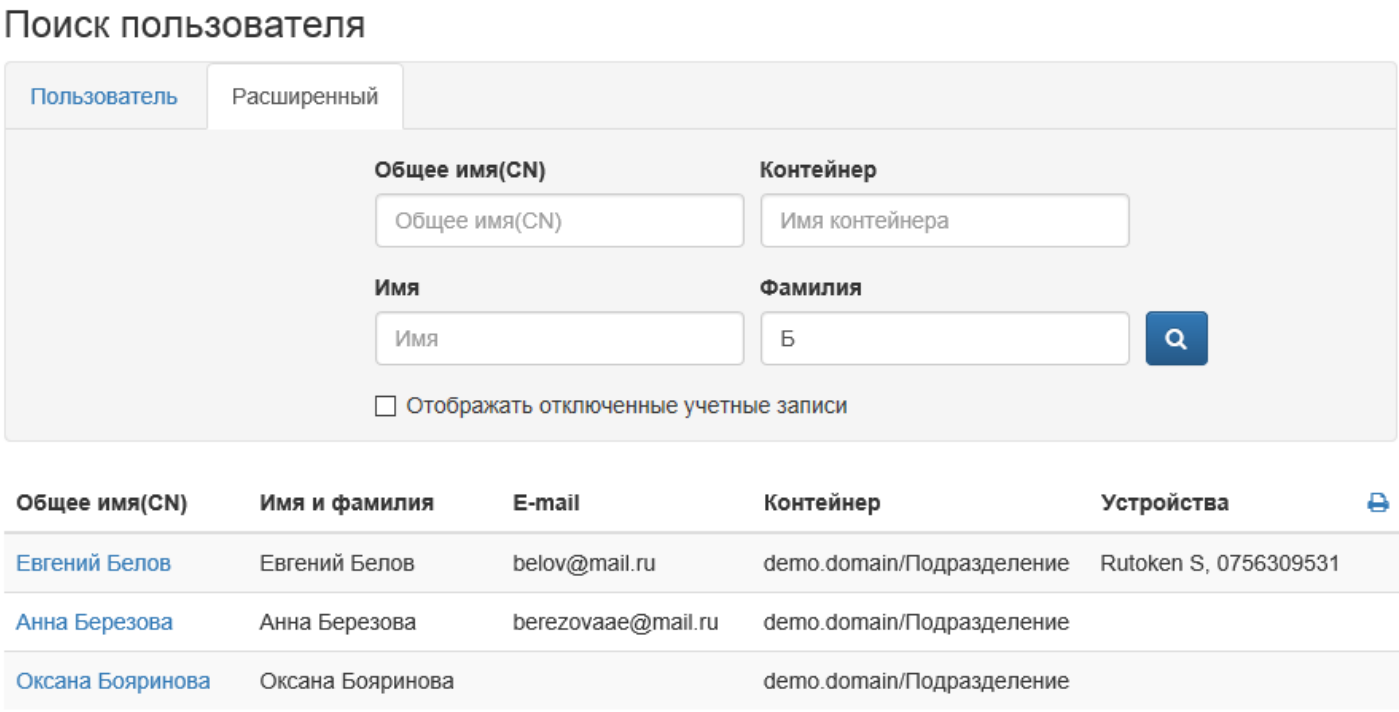

Рисунок 50 – Расширенный поиск пользователя.

При включенной опции **Отображать отключенные учетные записи** в результатах поиска будут отображены активные и отключенные учетные записи пользователей Active Directory. Переход к просмотру свойств пользователя (Карточке пользователя) осуществляется по щелчку на общее имя (CN) пользователя в результатах поиска. Результаты поиска пользователей могут быть сохранены в виде файла. Для создания файла с результатами поиска нажмите  и выберите формат. Сохраните полученный файл.

Карточка пользователя

В карточке пользователя содержится общая информация о пользователе: данные из профиля Active Directory[15], сведения по устройствам, средствам криптографической защиты информации (СКЗИ) и последние события пользователя (Рисунок 51). Если устройств у пользователя нет, оператор службы поддержки сможет их ему назначить или выпустить.

[15]В случае использования Active Directory в качестве каталога пользователей Indeed CM.

Евгений Белов

Логин	Евгений Белов
Путь	indeed-id.local/Indeed Company/Office/Headquarter/Евгений Белов
Политика	Headquarter
E-mail	belov@indeed.ru
Телефон	+7 (905) 2885823

Загрузить фотографию | Пользователь КриптоПро 2.0 | Сбросить ответы на секретные вопросы | Сбросить пароль пользователя

Назначенные устройства

Нет назначенных устройств

Выпустить устройство | Назначить устройство

Назначенные СКЗИ

Нет назначенных СКЗИ

Добавить СКЗИ | Редактировать СКЗИ | Уничтожить/изъять СКЗИ

Последние события

	Время	Событие	Сервис	Тип устройства	Серийный номер	Инициатор
▸	30.03.2017 12:20:46	Отвязка устройства	Консоль управления	Rutoken S	0783311611	INDEED-ID\ivan.ivanov
▸	30.03.2017 12:20:46	Очистка устройства	Консоль управления	Rutoken S	0783311611	INDEED-ID\ivan.ivanov
▸	30.03.2017 12:19:45	Отзыв устройства	Консоль управления	Rutoken S	0783311611	INDEED-ID\ivan.ivanov
▸	20.03.2017 18:17:02	Выпуск устройства	Консоль управления	Rutoken S	0783311611	INDEED-ID\ivan.ivanov
▸	13.02.2017 12:40:36	Отвязка устройства	Консоль управления	eToken PRO Java 72K	0210e19d	INDEED-ID\ivan.ivanov

Просмотреть все

Рисунок 51 – Карточка пользователя.

Загрузка фотографии. Если профиль пользователя в Active Directory содержит фотографию, то она будет отображена в карточке пользователя. Для загрузки фотографии вручную нажмите **Загрузить фотографию**.

Фотография пользователя может быть записана в атрибуты **thumbnailPhoto**[16] или **jpegPhoto**. Выбор атрибута осуществляется в Мастере настройки Indeed CM.[17]

Связь пользователя Indeed CM с каталогом УЦ. Если в используемой вами конфигурации каталог пользователей Indeed CM не совпадает с каталогом пользователей удостоверяющего центра (например, пользователям Active Directory необходимо выпускать сертификаты КриптоПро УЦ 2.0), то для выпуска устройства необходимо установить связь с каталогом нужного удостоверяющего центра.
Необходимость привязки пользователя к каталогу удостоверяющего центра определяется в политике использования устройств (раздел **Удостоверяющие центры**, опция **Устанавливать привязку между пользователем УЦ и пользователем каталога**). Один и тот же пользователь Active Directory может быть связан с каталогами различных УЦ.
Пользователь Indeed CM (не важно, в каком каталоге он расположен: Active Directory или КриптоПро 2.0) может быть связан с любым пользователем удостоверяющего центра КриптоПро 2.0. Если каталог УЦ, с которым необходимо установить связь, не содержит пользователей, то при помощи Indeed CM их можно создать.

Связать пользователя Active Directory с пользователем КриптоПро УЦ 2.0 можно автоматически (см. опцию Устанавливать привязку между пользователем УЦ и пользователем каталога) и в ручном режиме.

Для установки связи вручную:

1. Перейдите в карточку пользователя.
2. Нажмите **Пользователь КриптоПро 2.0** (Рисунок 52):

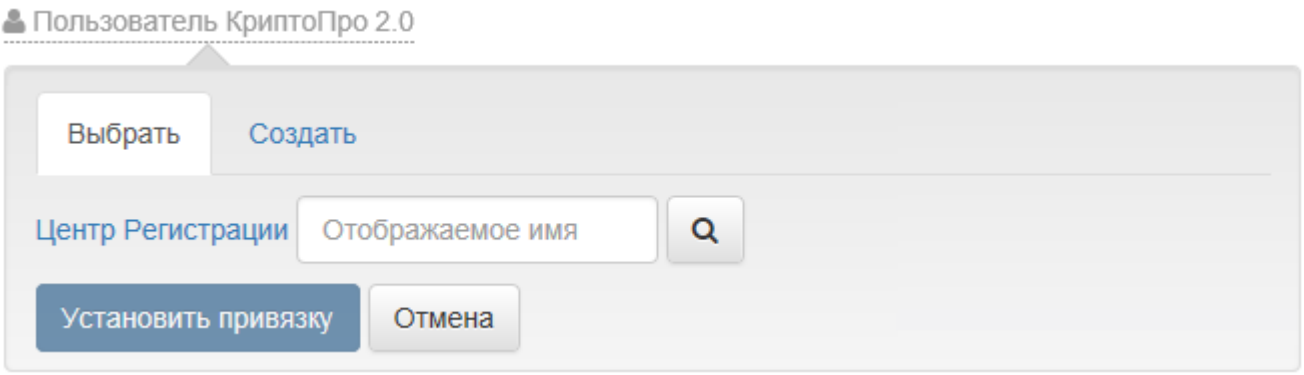

Рисунок 52 – Связывание пользователя Indeed CM с каталогом КриптоПро УЦ 2.0.

[16] Размер загружаемой фотографии не должен превышать 100Кб.
[17] Сервисная учетная запись должна обладать правами на запись для выбранного атрибута (см. **Работа с Microsoft Enterprise CA** в документе *Indeed CM. Руководство по установке и настройке*).

3. Введите имя пользователя центра регистрации КриптоПро УЦ 2.0 и укажите папку, в которой располагаются пользователи (Рисунок 53):

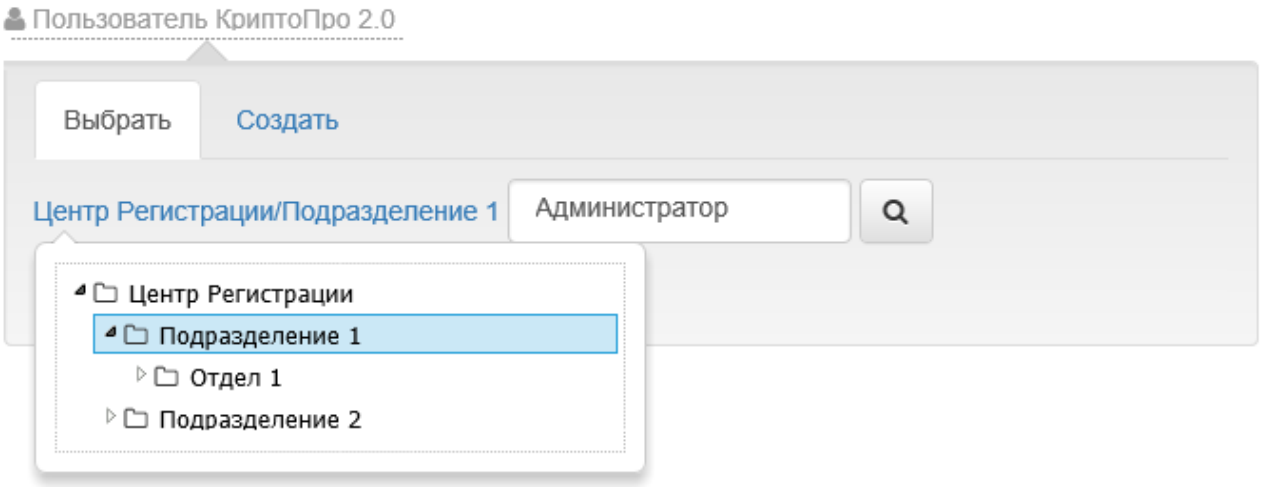

Рисунок 53 – Выбор папки в Центре Регистрации КриптоПро УЦ 2.0.

4. Нажмите кнопку поиска.

5. Отметьте нужного пользователя в результатах поиска и нажмите **Установить привязку** (Рисунок 54).

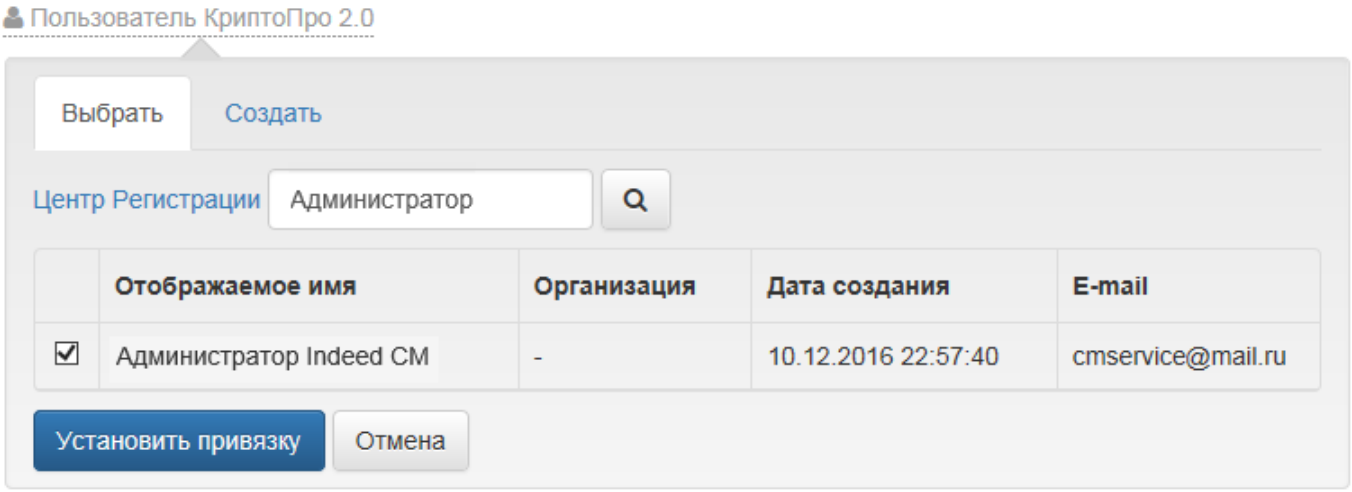

Рисунок 54 – Поиск пользователя каталога КриптоПро УЦ 2.0.

6. Установленную привязку можно отменить. Для этого нажмите **Пользователь КриптоПро 2.0** и затем **Отменить привязку** (Рисунок 55).

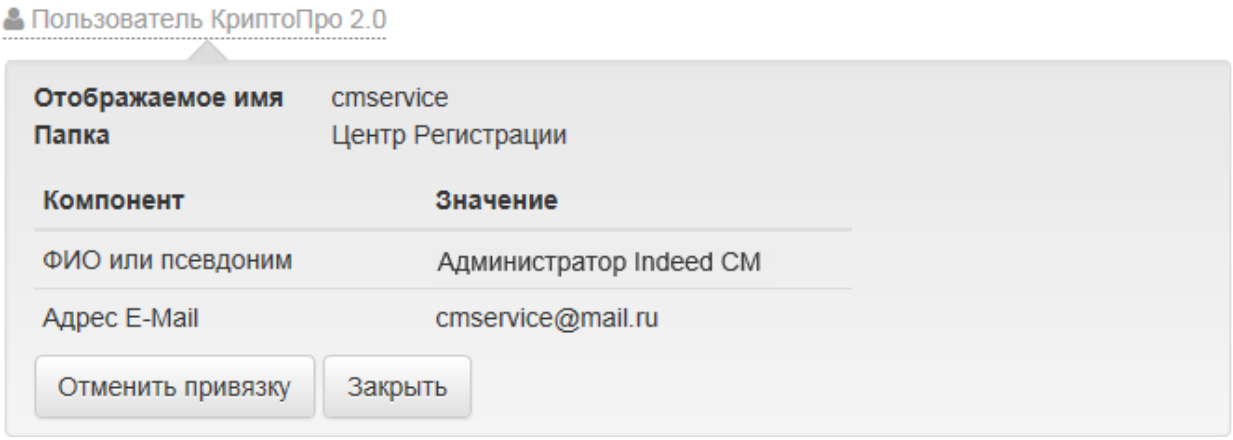

Рисунок 55 – Отмена привязки пользователя.

Для создания нового пользователя в каталоге КриптоПро УЦ 2.0:

1. Перейдите в карточку пользователя.
2. Нажмите **Пользователь КриптоПро 2.0** и перейдите на вкладку **Создать**. Вы можете отредактировать данные создаваемого пользователя. Перечень полей для редактирования, зависит от настроек используемого удостоверяющего центра КриптоПро (Рисунок 56).

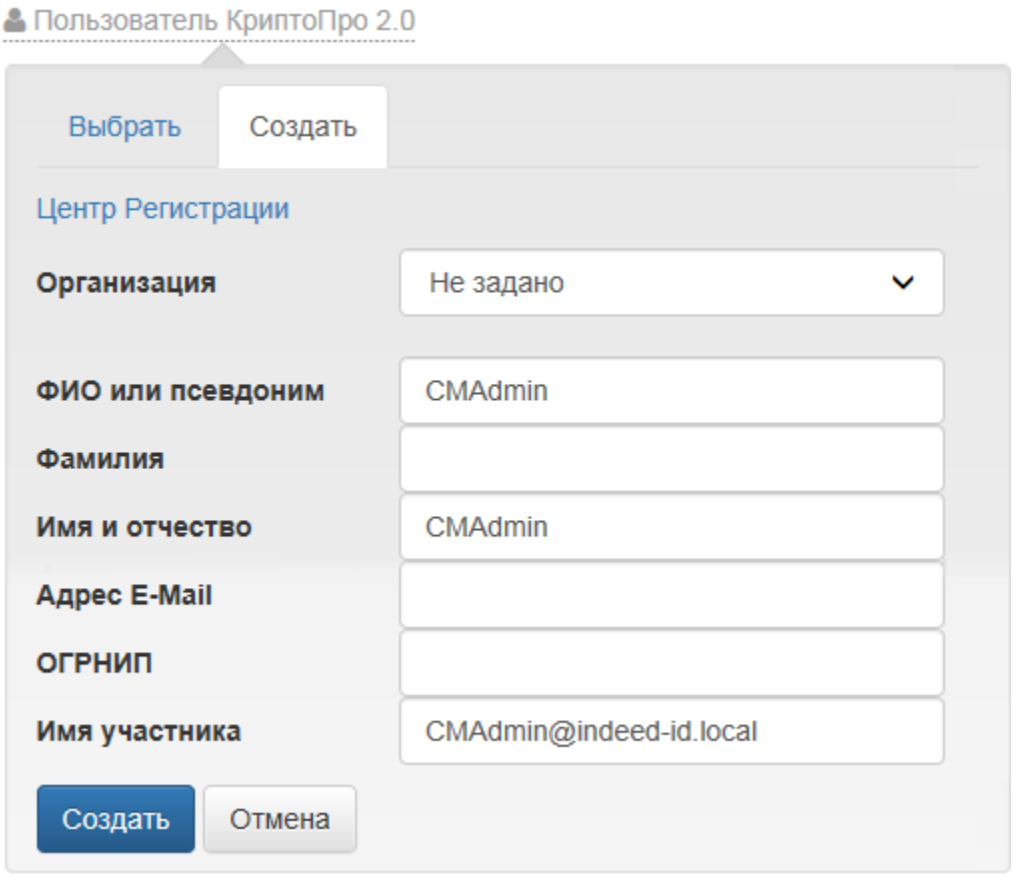

Рисунок 56 – Создание пользователя КриптоПро УЦ 2.0.

При создании пользователя КриптоПро УЦ 2.0 некоторые поля свойств могут быть заполнены автоматически. Например, имя пользователя, адрес электронной почты, город, страна, организация. Эти данные Indeed CM получает из профиля пользователя Active Directory (см. раздел **Соответствия атрибутов** в **Мастере настройки Indeed CM**) или из шаблона организации (см. Организации в политике использования устройств).

Сброс ответов на секретные вопросы. Оператор Indeed CM при необходимости может сбросить секретные вопросы пользователя и указанные ответы. В этом случае пользователь должен будет установить новые вопросы и задать ответы в приложении Self Service.
Для сброса секретных вопросов пользователя:

1. В карточке пользователя нажмите **Сбросить ответы на секретные вопросы**.
2. Нажмите **Сбросить** для подтверждения действия.

Сброс пароля пользователя. Indeed CM позволяет операторам и администраторам выполнить сброс доменного пароля пользователя. Сброс доменного пароля может использоваться в случае возникновения необходимости входа пользователя в операционную систему по паролю. Например, если он забыл смарт-карту с сертификатом для аутентификации и не знает свой доменный пароль. Для сброса пароля нажмите **Сбросить пароль пользователя**, задайте новое значение, опцию смены при первом входе (если необходимо) и время истечения срока действия пароля (Рисунок 57):

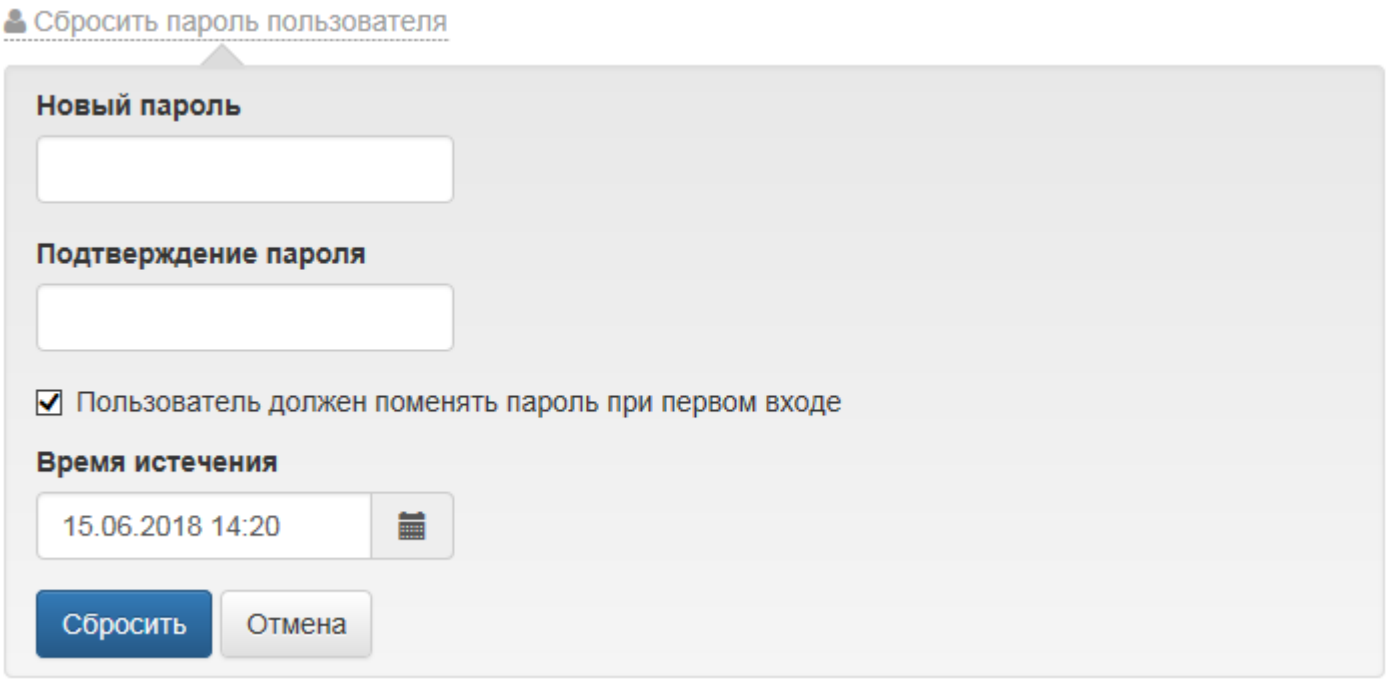

Рисунок 57 – Сброс доменного пароля пользователя.

Сервисная учетная запись должна обладать правами на сброс пароля в Active Directory (см. **Создание учетной записи для работы с хранилищем данных Indeed CM** в документе *Indeed CM. Руководство по установке и настройке*).

Время истечения – значение, после которого пароль будет сброшен на случайное значение приложением Card Monitor. Пароль будет состоять из:

- латинских строчных и прописных букв
- цифр
- 10 символов

Установленный пароль не будет записан в хранилище Indeed CM.

Назначение устройства. Назначение устройства пользователю заключается в том, что устройство присваивается указанному пользователю, для того, чтобы он в последствии самостоятельно его выпустил при помощи приложения Self Service.

Одно устройство может одновременно принадлежать только одному пользователю. У одного пользователя может быть несколько устройств. Возможность пользователей самим назначать себе устройства задается администратором в меню **Поведение** созданной политики в разделе **Конфигурация**.

Для назначения устройства пользователю выполните следующие действия:

1. Перейдите в карточку пользователя и нажмите **Назначить устройство**.
2. Если устройство доступно, подключите его к компьютеру.
3. Если PIN-код администратора не соответствует значению, заданному производителем (или значению, указанному в **Типе устройства**), то укажите PIN-код администратора для каждой области в разделе **Дополнительно** и нажмите **Назначить** (Рисунок 58).

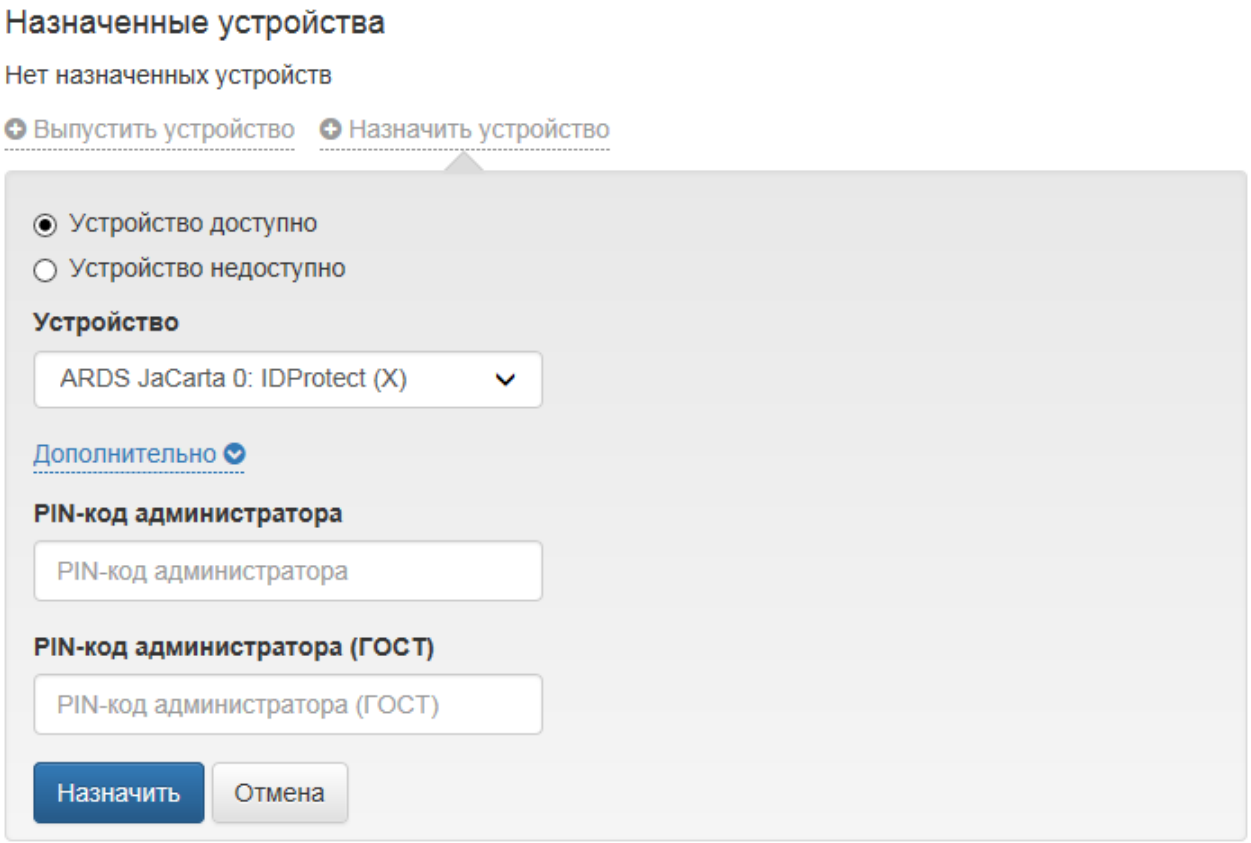

Рисунок 58 – Назначение доступного устройства.

4. Если устройство недоступно, но известны его серийный номер и тип, укажите их и нажмите **Назначить** (Рисунок 59).

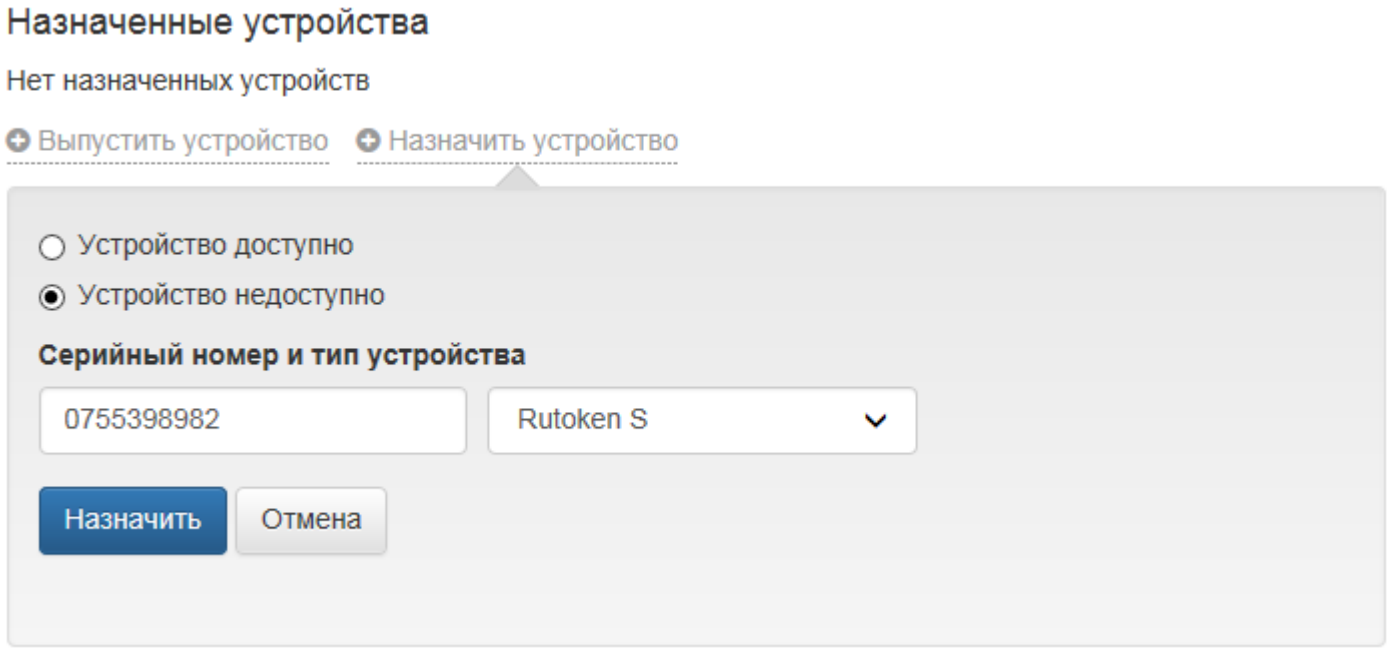

Рисунок 59 – Назначение недоступного устройства.

5. Назначенное устройство имеет статус **Назначено** в карточке пользователя.

Отмена назначения устройства
Назначенное пользователю, но ещё не выпущенное устройство можно отозвать. Для отмены назначения устройства перейдите на карточку пользователя, выберите назначенное устройство и нажмите **Отвязать**. Подтвердите действие нажатием кнопки **Отвязать**.

Выпуск устройства. Во время процедуры выпуска устройство персонализируется для пользователя: в соответствии с настройками назначенной политики использования устройств осуществляется инициализация устройства, генерируются ключевые пары, выпускаются необходимые сертификаты и происходит их запись в память устройства.

Создание запроса сертификата и запись на устройство происходят в следующем порядке:

1. Генерируется пара ключей на клиентской стороне с использованием криптопровайдера (CSP).
2. Формируется запрос на сертификат, в который вкладывается открытый ключ пользователя.
3. Запрос подписывается закрытым ключом пользователя.
4. Запрос подписывается ключом сервисной учетной записи оператора УЦ с необходимыми правами, которым владеет сервер системы Indeed CM.
5. Запрос отправляется на удостоверяющий центр.
6. Выпущенный сертификат записывается на носитель средствами криптопровайдера.

Для выпуска устройства пользователю выполните следующие действия:

1. Перейдите на вкладку **Пользователи** и выполните поиск пользователя.

2. Перейдите в карточку пользователя, щелкнув по его логину в результатах поиска.
3. Нажмите **Выпустить устройство**.

Если политика использования устройств позволяет выбирать сертификаты для записи на устройство (см. опцию **Необязательный сертификат** в параметрах шаблона сертификата политики использования устройств Indeed CM), то такие сертификаты необходимо указать и нажать **Далее** (Рисунок 60).

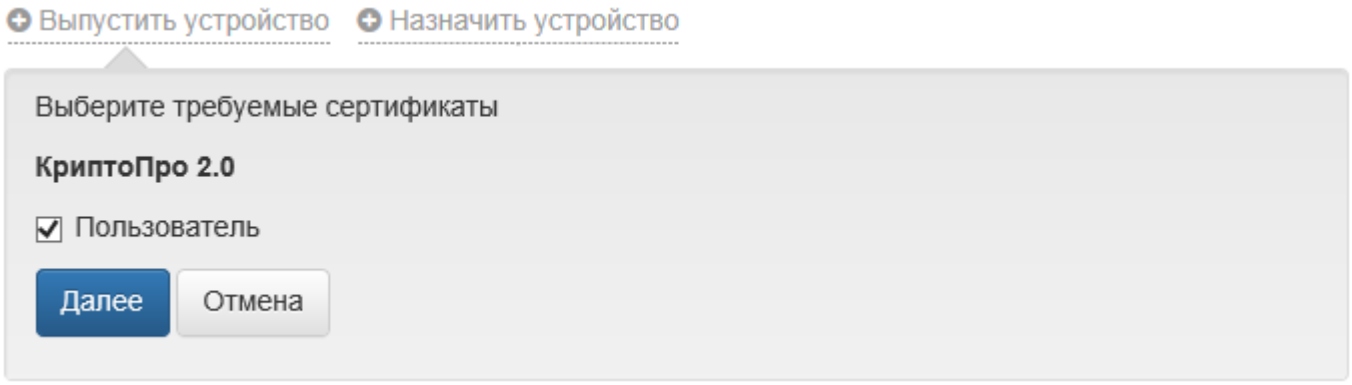

Рисунок 60 – Выбор сертификатов для записи на устройство.

4. Подключите устройство к компьютеру, задайте его имя[18] и, при необходимости введите:
   - **PIN-коды администратора** (если устройство не добавлено в Indeed CM) и пользователя в разделе **Дополнительно**.
     Значения PIN-кода пользователя и администратора могут быть пустыми. В этом случае они будут установлены в соответствии со значением в разделе **Конфигурация – Типы устройств**. Поддерживается ввод PIN-кодов для нескольких областей (например, для PKI и ГОСТ на устройствах JaCarta).
   - **Комментарий к устройству**
     При включенной опции **Использовать комментарий устройства в качестве комментария пользователя к запросу на сертификат** в шаблоне сертификата КриптоПро УЦ 2.0 текст комментария будет добавлен в запрос.

   Для выпуска устройства нажмите **Выпустить** (Рисунок 61).

[18]Имя устройства может быть подставлено автоматически. См. Настройки выпуска устройства.

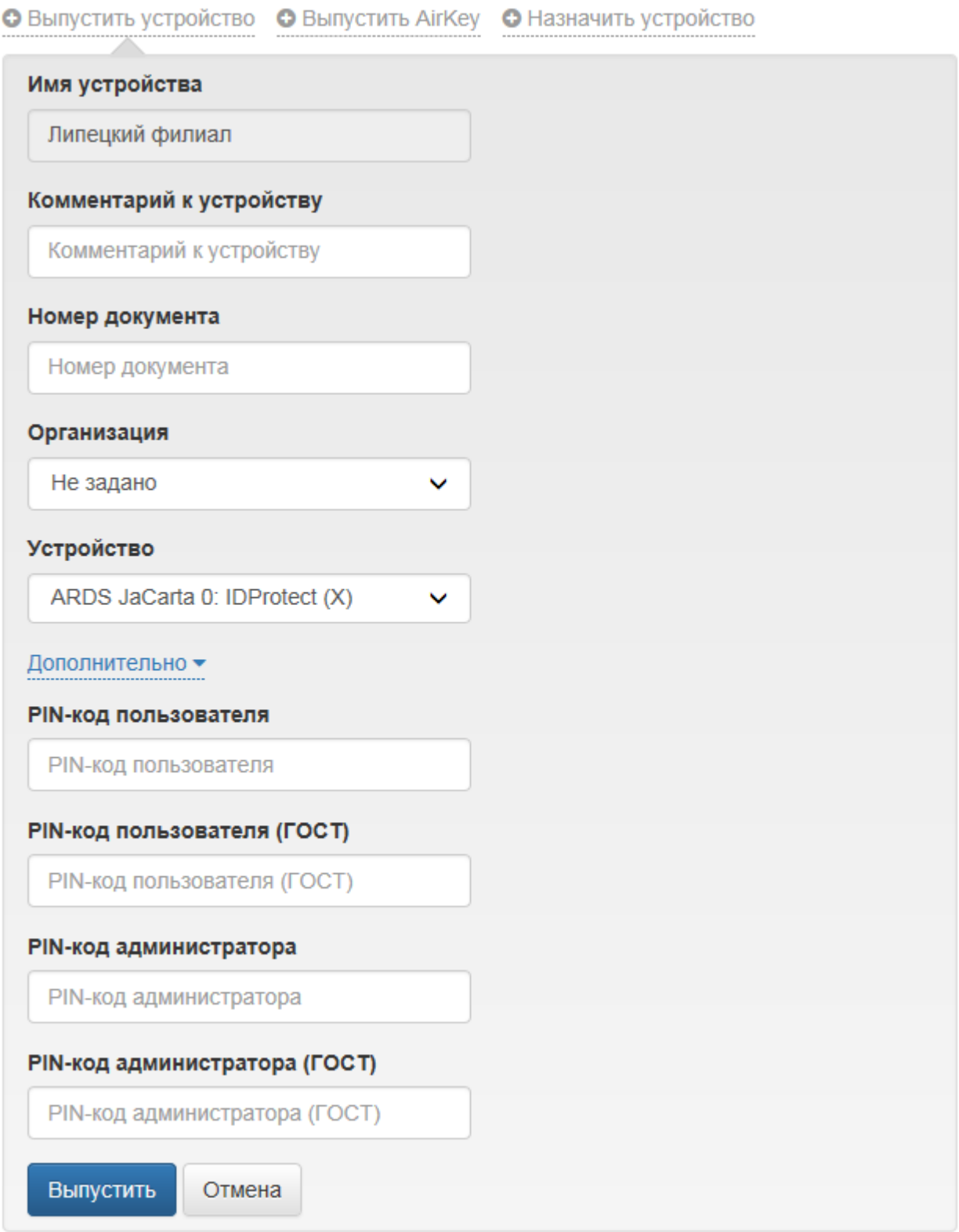

Рисунок 61 – Выпуск устройства с установкой PIN-кода пользователя вручную.

5. Если ведется учет СКЗИ, то в пункте **Номер документа** укажите номер документа (приказа, распоряжения), в соответствии с которым пользователю создается СКЗИ.

Информация об имеющихся у пользователя СКЗИ находится в разделе **Назначенные СКЗИ** карточки пользователя.

6. Выберите **Организацию** пользователя, если Indeed CM использует данные шаблона организации для создания пользователя в каталоге Центра Регистрации КриптоПро УЦ 2.0.
7. Если в политике использования устройств включена инициализация устройства, то в процессе выпуска отобразится соответствующее уведомление (Рисунок 62).

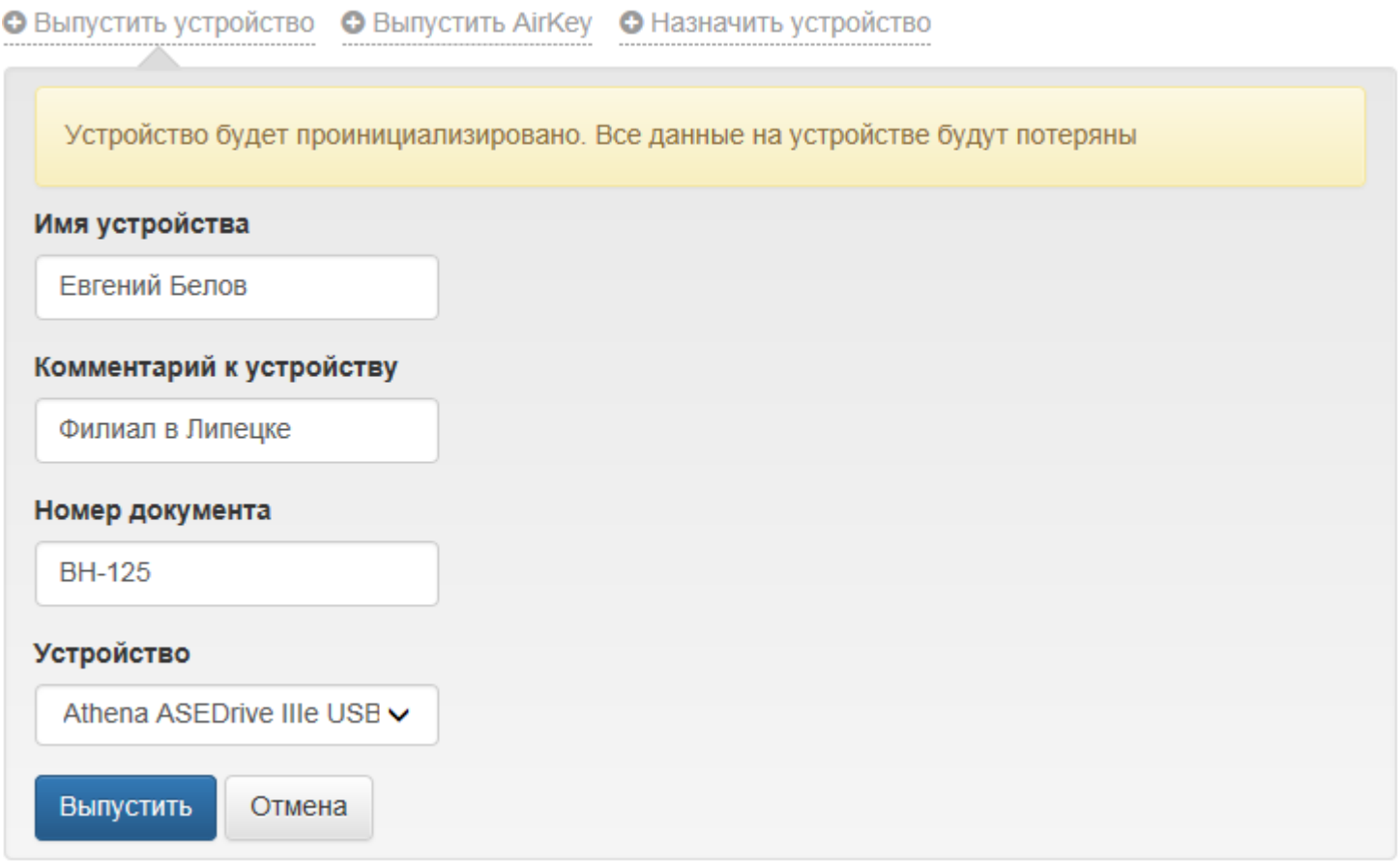

Рисунок 62 – Выпуск устройства.

8. После выпуска устройства в разделе **Назначенные устройства** карточки пользователя отобразятся сведения об устройстве (Рисунок 63):
   - Тип и серийный номер
   - Имя (если было указано)
   - Комментарий (если был указан)
   - Имя политики, с параметрами которой выпущено устройство
   - PIN-код администратора[19]
   - Состояние (в ожидании, выпущено, выключено, отозвано)
   - Записанные сертификаты: шаблон, имя центра сертификации, выдавшего сертификат, срок действия и текущее состояние

[19] Доступно при включении опции **Разрешить операторам просматривать административный PIN-код устройства** в Мастере настройки Indeed CM в разделе **Функции системы**.

Для установки или изменения комментария нажмите ✎, для отображения PIN-кода администратора нажмите 👁.

Просмотр PIN-кода администратора устройства доступен только пользователям с правами Indeed CM Admins.

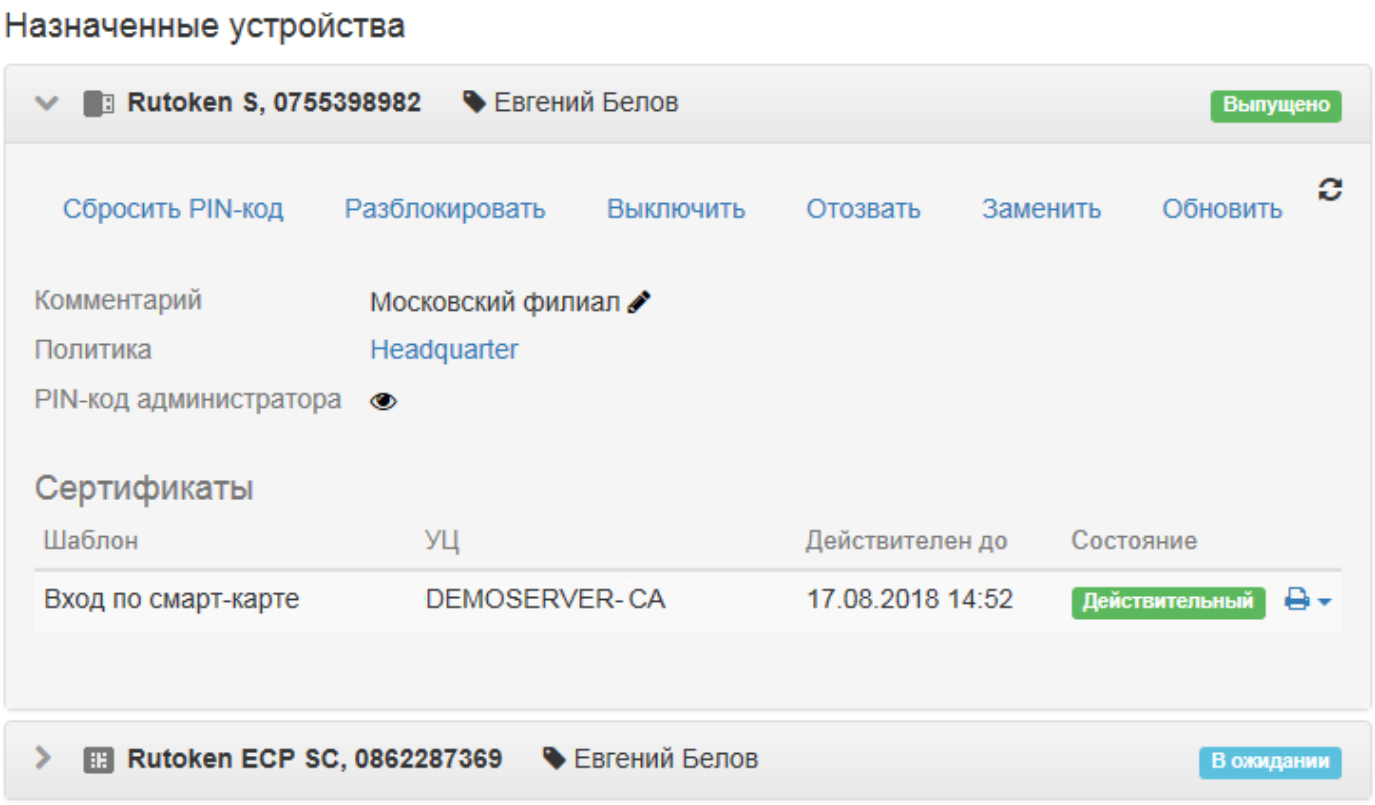

Рисунок 63 – Устройства пользователя.

В Таблице 7 содержатся все возможные состояния сертификатов, закрытых ключей, запросов на сертификаты и их описание.

Таблица 7 – Состояния сертификатов.

Состояние сертификата	**Описание**
Действительный	Срок действия сертификата еще не истек. Сертификат пригоден для использования.
Отозван	Сертификат отозван. Отзыв может быть временным или окончательным. В случае **временного отзыва** (в результате выключения устройства), срок действия сертификата приостанавливается на период выключения устройства. После включения устройства сертификат снова становится действительным (если его срок действия не истек пока устройство было выключено). В случае **окончательного отзыва** (в результате отзыва устройства или его изъятия), сертификат более не может использоваться.
Истекает	Срок действия сертификата скоро закончится. Выполните обновление сертификата, если планируется его дальнейшее использование.
Ключ истекает	Срок действия закрытого ключа сертификата, выданного КриптоПро УЦ скоро закончится. Выполните обновление сертификата, если планируется его дальнейшее использование. Закрытый ключ в этом случает также будет обновлен.
Истек	Срок действия сертификата истек. Сертификат не пригоден для использования. Срок действия сертификата может быть продлен на период равный сроку его действия, заданный в шаблоне сертификата (см. Обновление устройства).
Ошибка	Состояние сертификата не удалось определить. Возможно, центр сертификации недоступен. Сертификат не пригоден для использования.
Одобрен	Запрос на сертификат одобрен администратором, но сертификат еще не выпущен пользователю.
Отклонен	Запрос на сертификат отклонён администратором.
В ожидании	Запрос на сертификат ожидает рассмотрения администратором.

Жизненный цикл устройств (смарт-карт) в системе Indeed CM представлен на Рисунке 64.

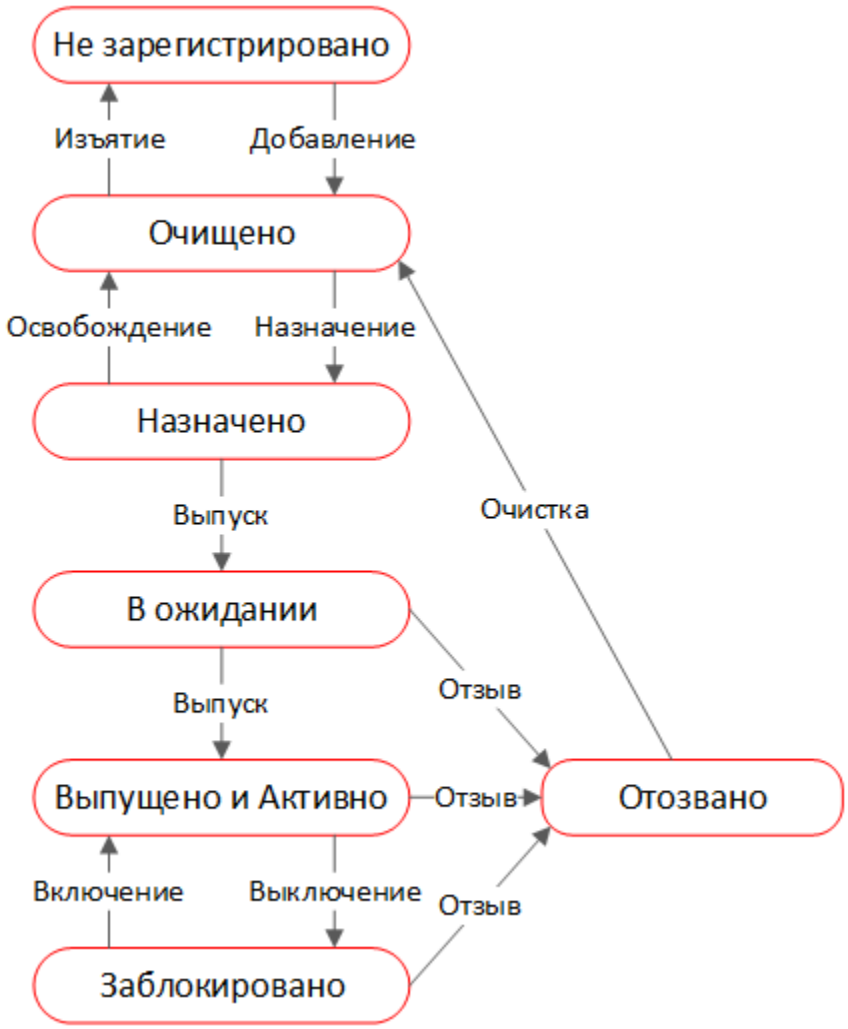

Рисунок 64 – Жизненный цикл устройств (смарт-карт) в системе Indeed CM.

Если запрос на сертификат пользователя требует одобрения оператора удостоверяющего центра, то текущее состояние этого запроса отобразится в карточке пользователя (Рисунок 65).

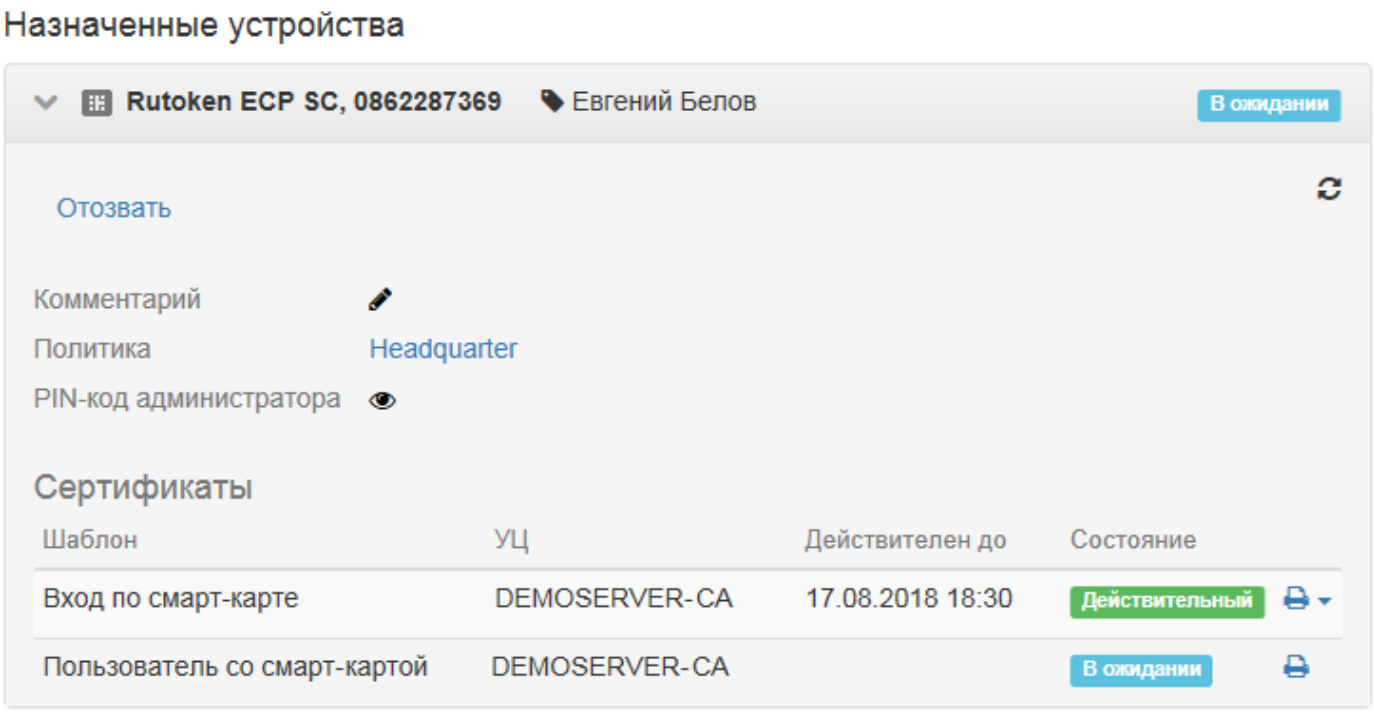

Рисунок 65 – Сертификат пользователя, ожидающий подтверждения.

После одобрения запроса на сертификат оператором удостоверяющего центра состояние запроса изменится на **Одобрен** (Рисунок 66). После чего выпуск устройства может быть продолжен (станет доступна кнопка **Продолжить выпуск**).

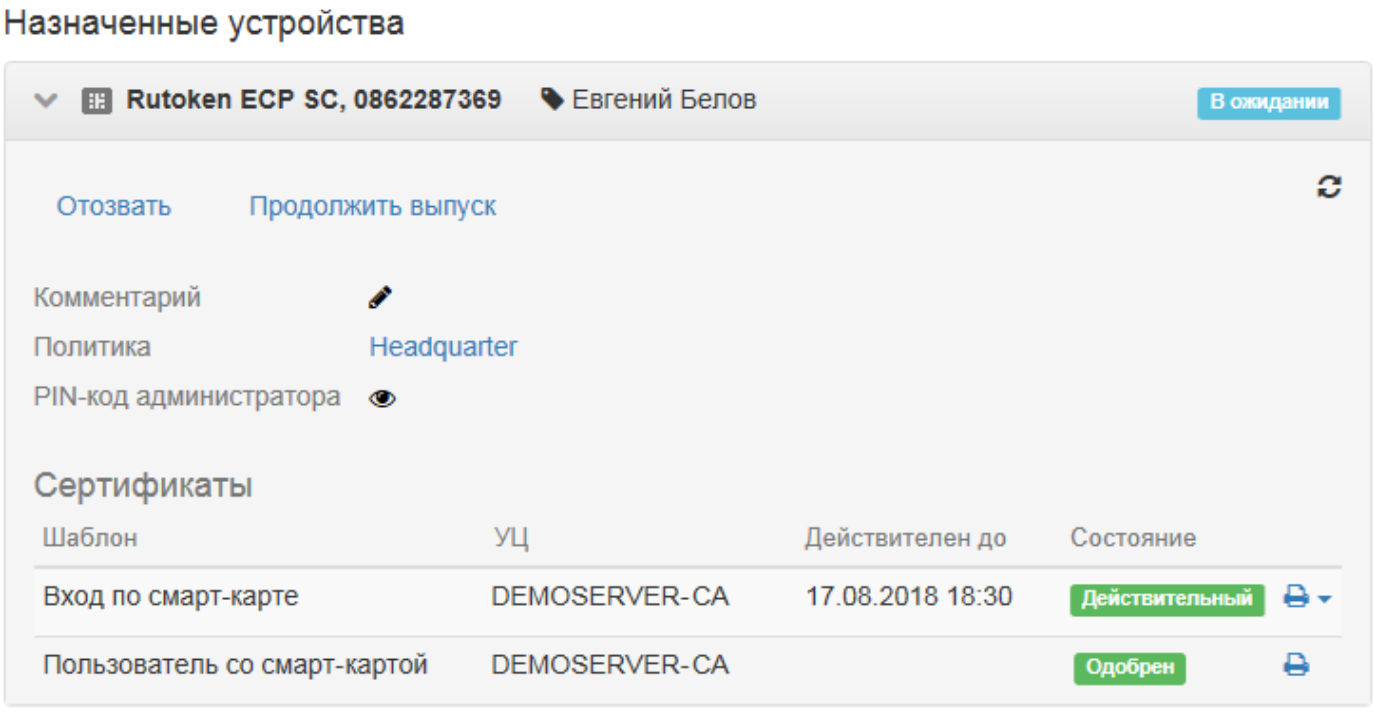

Рисунок 66 – Сертификат пользователя, одобренный оператором УЦ.

Даже если один из сертификатов был автоматически одобрен (находится в состоянии **Действительный**), он будет записан на устройство только после нажатия на **Продолжить выпуск**.
Выпуск устройства невозможен, пока оператором УЦ не будет одобрен каждый запрос на сертификат.

По завершению процесса выпуска устройства будет отображен случайный PIN-код пользователя если политика выпуска устройства предполагает создание случайного PIN-кода и его отображение в момент выпуска (Рисунок 67). Установленный PIN-код пользователя может быть отправлен на электронную почту пользователя и/или его руководителя (см. уведомление пользователя **Установка PIN-кода**) или напечатан на конверте.

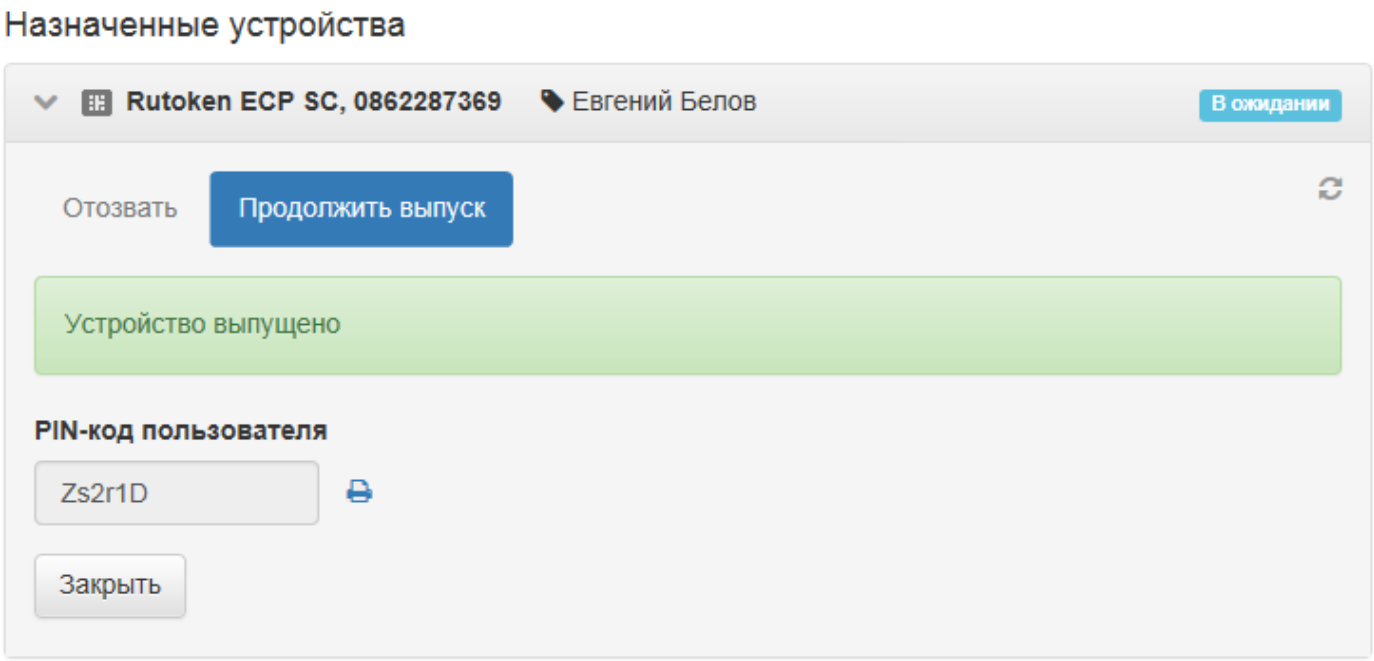

Рисунок 67 – Случайный PIN-код пользователя.

Для печати PIN-кода нажмите . Страница печати откроется в новой вкладке (Рисунок 68).

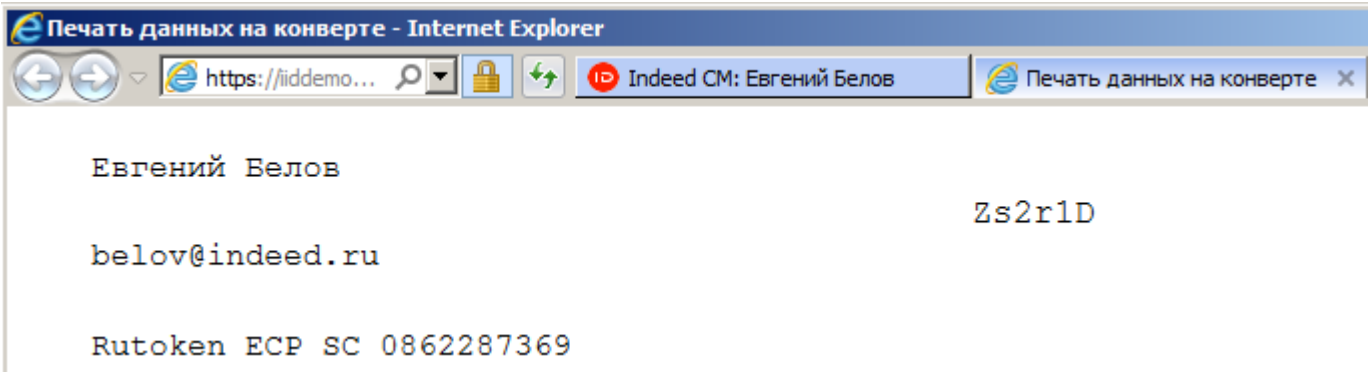

Рисунок 68 – Страница печати PIN-кода пользователя.

Параметры печати содержатся в шаблоне C:\inetpub\wwwroot\icm\Content\pinenvelope.xsl. По умолчанию на печать выводится информация о пользователе (имя и email) и устройстве (тип, серийный номер и PIN-код пользователя). Для изменения шаблона печати отредактируйте файл pinenvelope.xsl.

Публикация выпущенных сертификатов
Выпущенные и записанные на устройство пользователя сертификаты в зависимости от настроек Indeed CM могут быть опубликованы в:

- Локальное хранилище сертификатов пользователя на рабочей станции[20]
- Файловое хранилище[21]

> Публикация сертификатов не поддерживается для примонтированных сетевых дисков. Задайте путь к файловому хранилищу в формате:
> `\\Имя рабочей станции\Имя сетевого каталога`

- Каталог пользователей в Active Directory[22]
- Базу приложений ЦФТ[23]

Печать персонального сертификата (запроса сертификата)
Запросы на сертификат и сами сертификаты выводятся на печать в интерфейсе Indeed CM. Для печати запроса или сертификата нажмите справа от запроса/сертификата. Страница печати откроется в новой вкладке браузера. Для изменения шаблона печати отредактируйте файлы консоли управления и сервиса самообслуживания.
Консоль управления:

- C:\inetpub\wwwroot\icm\Content\request.xsl – шаблон печати запроса
- C:\inetpub\wwwroot\icm\Content\cert.xsl – шаблон печати сертификата

Сервис самообслуживания:

- C:\inetpub\wwwroot\icmservice\Content\request.xsl – шаблон печати запроса
- C:\inetpub\wwwroot\icmservice\Content\cert.xsl – шаблон печати сертификата

Сброс PIN-кода. Оператор Indeed CM может сбросить PIN-код устройства пользователя. В этом случае PIN-код, заданный пользователем, изменяется на значение, указанное в разделе **Тип устройства**. Для сброса PIN-кода пользователя выполните следующие действия:

1. Перейдите на вкладку **Пользователи** и выполните поиск пользователя.
2. Перейдите в карточку пользователя, щелкнув по его логину в результатах поиска.

[20]Опция **Устанавливать сертификат в локальное хранилище** в свойствах шаблона сертификата в политике использования устройств.
[21]Опция **Публиковать сертификаты пользователей КриптоПро УЦ 2.0 в файловое хранилище.**
[22]Опция **Публиковать сертификат в каталоге пользователей** в свойствах шаблонов КриптоПро УЦ 2.0 в политике использования устройств.
[23]Опция **Публиковать сертификат в ЦФТ** в свойствах шаблонов КриптоПро УЦ 2.0 в политике использования устройств.

3. Выберите нужное устройство и раскройте информацию о нем.
4. Нажмите **Сбросить PIN-код**.
5. Подключите устройство и нажмите **Сбросить**.

После сброса PIN-кода администратором, пользователь сможет задать новый PIN-код самостоятельно, при помощи приложения Self Service.

Разблокировка устройства. В случае, если пользователь ввел неверный PIN-код устройства больше определенного количества раз, оно блокируется.
Максимальное количество попыток ввода PIN-кода пользователем задается администратором в политике использования устройства в разделе **Инициализация устройства**. Существует два режима разблокировки устройства пользователя: online и offline.

Разблокировка устройства (смарт-карты, usb-токена) на экране входа в Windows не поддерживается при удаленном подключении через Remote Desktop.

Online-разблокировка осуществляется пользователем в интерфейсе операционной системы. Пользователь отвечает на секретные вопросы, задает и подтверждает новый PIN-код, после чего устройство разблокируется. Для online-разблокировки обязательным условием является наличие соединения рабочей станции пользователя, к которой подключено заблокированное устройство, с сервером Indeed CM. На Рисунке 69 приведен пример online-разблокировки устройства в интерфейсе операционной системы Windows 8. Механизм разблокировки устройства в операционных системах Windows 7 и Windows 10 выглядит похожим образом.

Если секретные вопросы пользователя не установлены, online-разблокировка устройства будет недоступна. Разблокировать устройство можно будет в режиме offline.

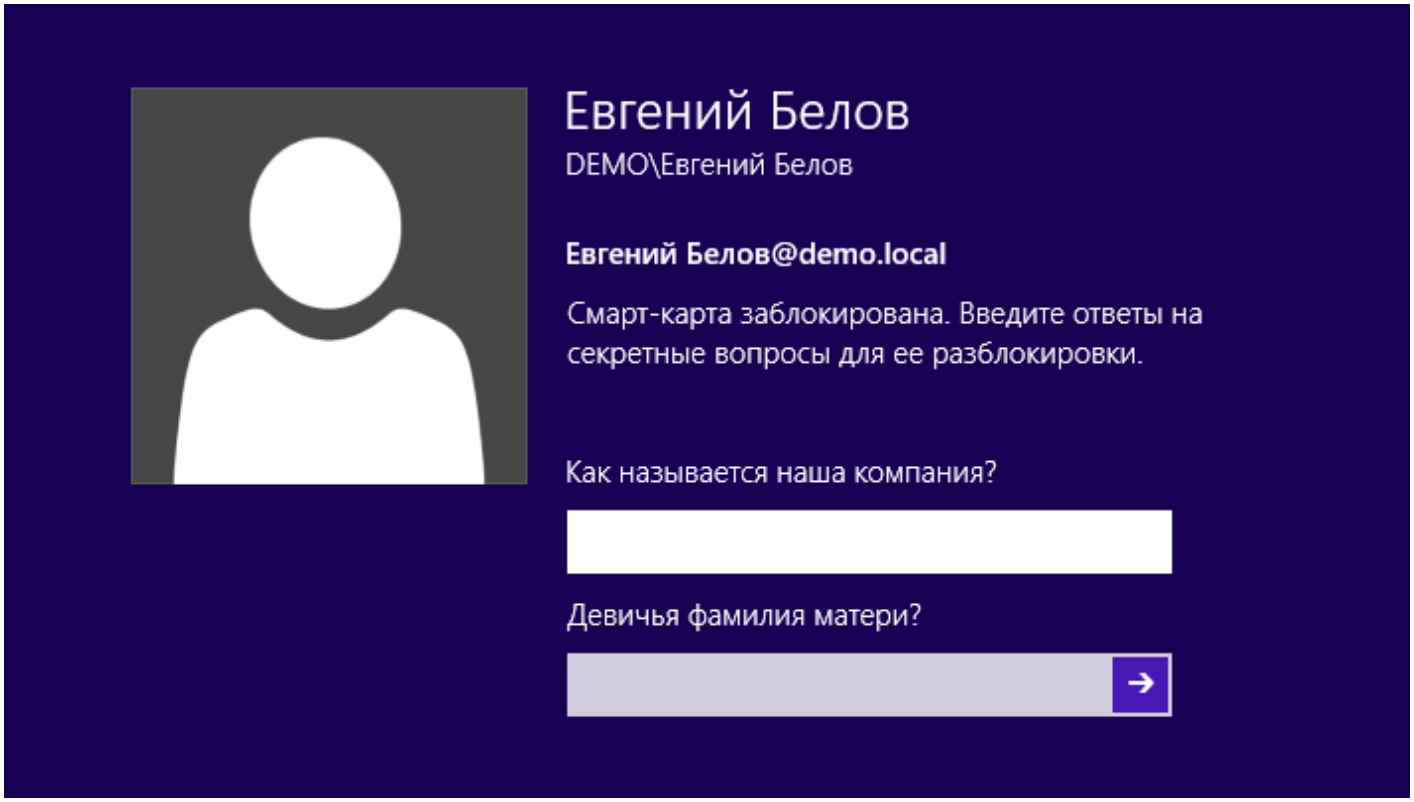

Рисунок 69 – Online разблокировка устройства в интерфейсе Windows 8.

Offline-разблокировка осуществляется оператором системы по принципу аутентификации вида запрос-ответ (англ. challenge-response authentication mechanism).
При исчерпании заданного числа попыток ввода PIN-кода, пользователь получает сообщение о том, что его устройство заблокировано. Вместе с сообщением пользователь получает уникальный 16-ти символьный код-запрос. Пользователю необходимо связаться с оператором системы (например, по телефону), подтвердить свою личность, ответив на секретные вопросы[24] и сообщить полученный код. На Рисунке 70 приведен пример экрана offline-разблокировки устройства в интерфейсе операционной системы Windows 8.
Оператор системы открывает карточку пользователя и в перечне действий над устройством выбирает пункт **Разблокировать**. Прежде, чем выполнить генерацию ответного кода для разблокировки устройства, администратор системы задает секретный вопрос (или несколько вопросов, в зависимости от настроек политики использования устройств) и вводит полученный от пользователя ответ в соответствующую форму (Рисунок 71).

Offline-разблокировка может быть отключена в политике использования устройств. В этом случае кнопка **Разблокировать** в карточке пользователя раздела **Пользователи** будет недоступна. Требование ответов на секретные вопросы может быть отключено в политике использования устройств.

[24]Необходимость ответов на секретные вопросы при offline-разблокировке определяется в опцией **Проверять ответы на секретные вопросы** в разделе **Поведение** политики использования устройств

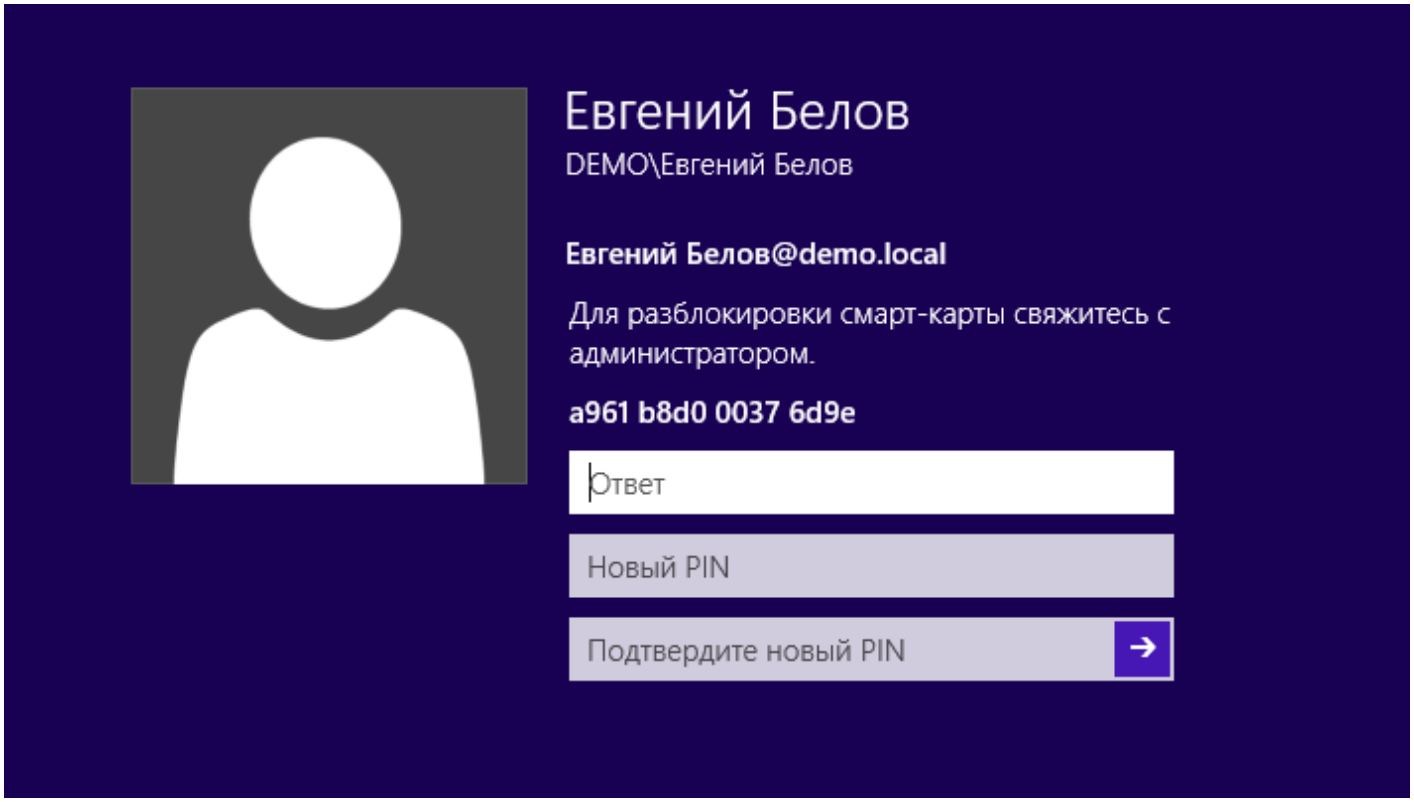

Рисунок 70 – Offline разблокировка устройства в интерфейсе Windows 8.

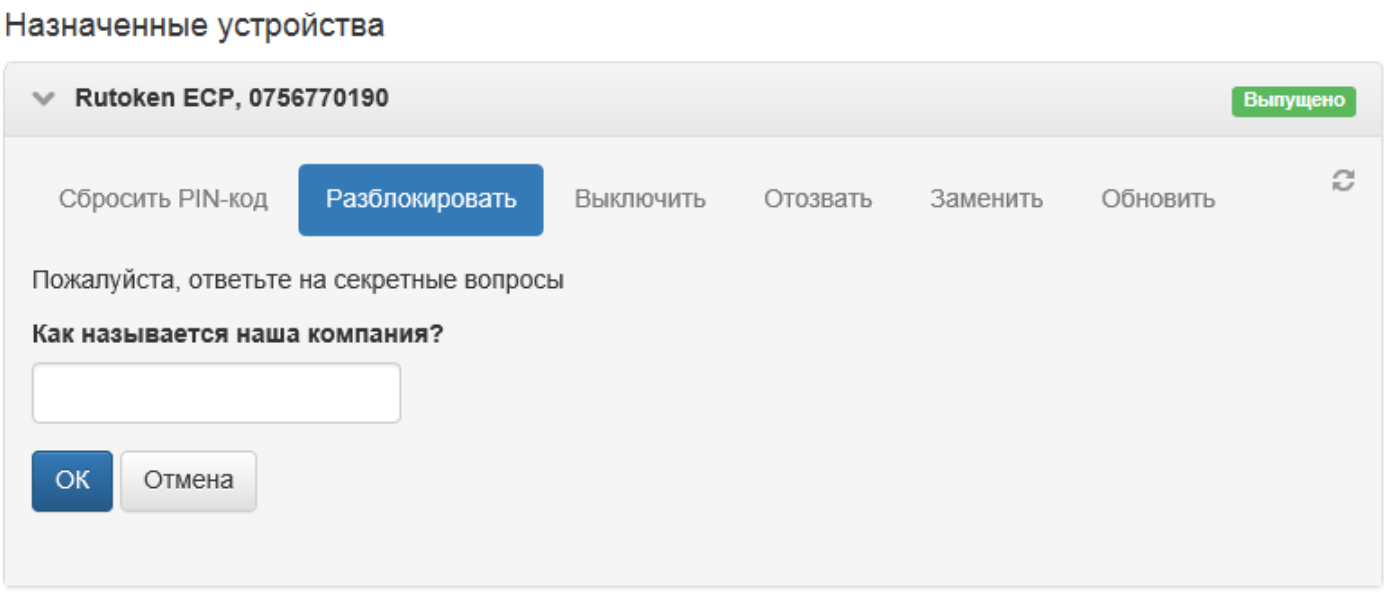

Рисунок 71 – Offline разблокировка устройства в интерфейсе оператора Indeed CM.

Если ответы на все вопросы даны верно, то оператор вводит код, который ему сообщает пользователь и система генерирует ответный код, который оператор сообщает пользователю (Рисунок 72). Пользователь вводит код, полученный от оператора, и задает новый PIN-код устройства. В случае успешной разблокировки отображается соответствующее сообщение.

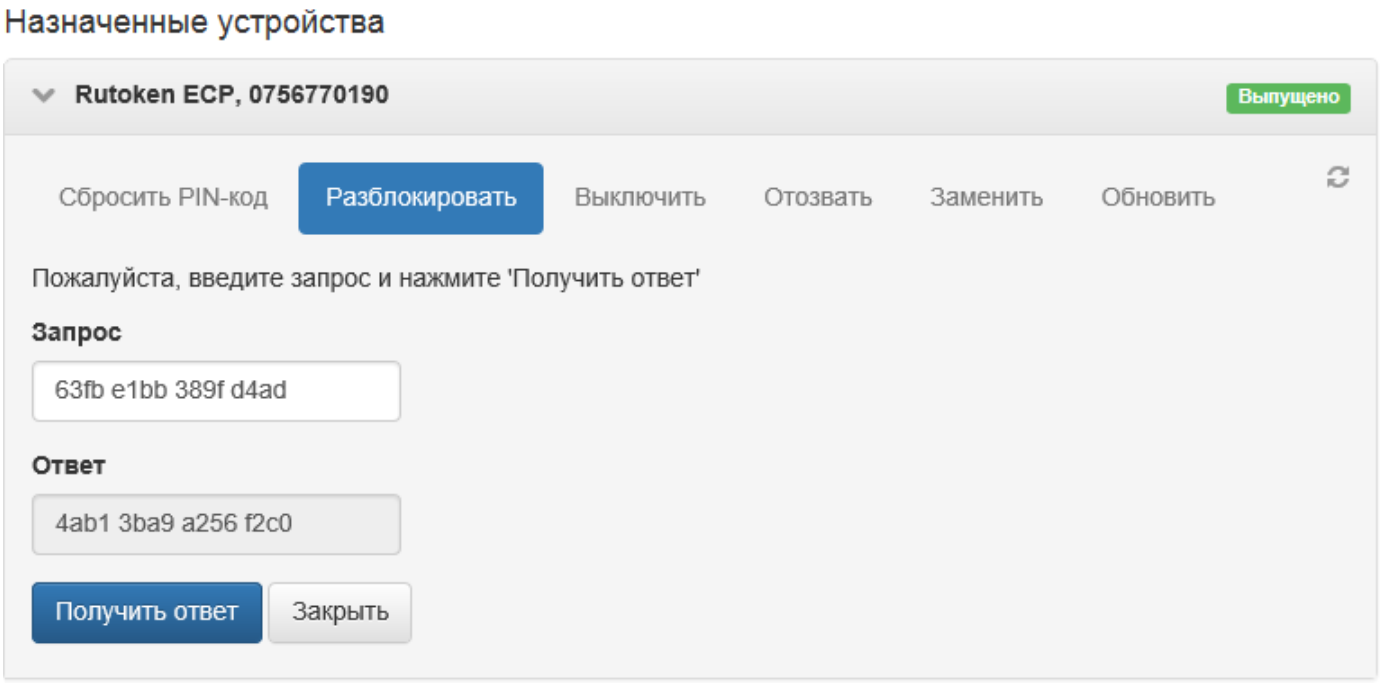

Рисунок 72 – Генерация ответного кода при offline разблокировке устройства.

Разблокировка устройства при помощи утилиты Indeed CM Unblock. Устройство пользователя может не использоваться для входа в операционную систему. В этом случае для его разблокировки применяется утилита **Indeed CM Unblock** (расположение по умолчанию: %ProrgamFiles%/Indeed CM/IndeedCM.Unblock.exe).
Механизм разблокировки устройства при помощи утилиты Indeed CM Unblock аналогичен механизму offline-разблокировки.

Выключение устройства без выполнения входа в систему. В экстренном случае пользователь может самостоятельно выключить устройство без выполнения входа в операционную систему.

Выключение устройства доступно только в том случае, если у рабочей станции, с которой осуществляется операция, есть связь с сервером Indeed CM и у пользователя настроены секретные вопросы.

Возможность выключения устройства может быть отключена для определенных категорий пользователей (см. раздел **Настройка online-разблокировки устройств** в документе *Indeed CM. Руководство по установке и настройке*).

Для выключения устройства выберите **Выключение смарт-карты** на экране выбора пользователей. На Рисунке 73 приведен пример для операционной системы Windows 8. Механизм выключения в операционных системах Windows 7 и Windows 10 выглядит похожим образом.
Укажите имя пользователя (логин), устройство (смарт-карту) которого необходимо выключить (Рисунок 74) и затем введите ответы на секретные вопросы (Рисунок 75). Выберите устройство из списка выпущенных устройств пользователя и нажмите → (Рисунок 76).

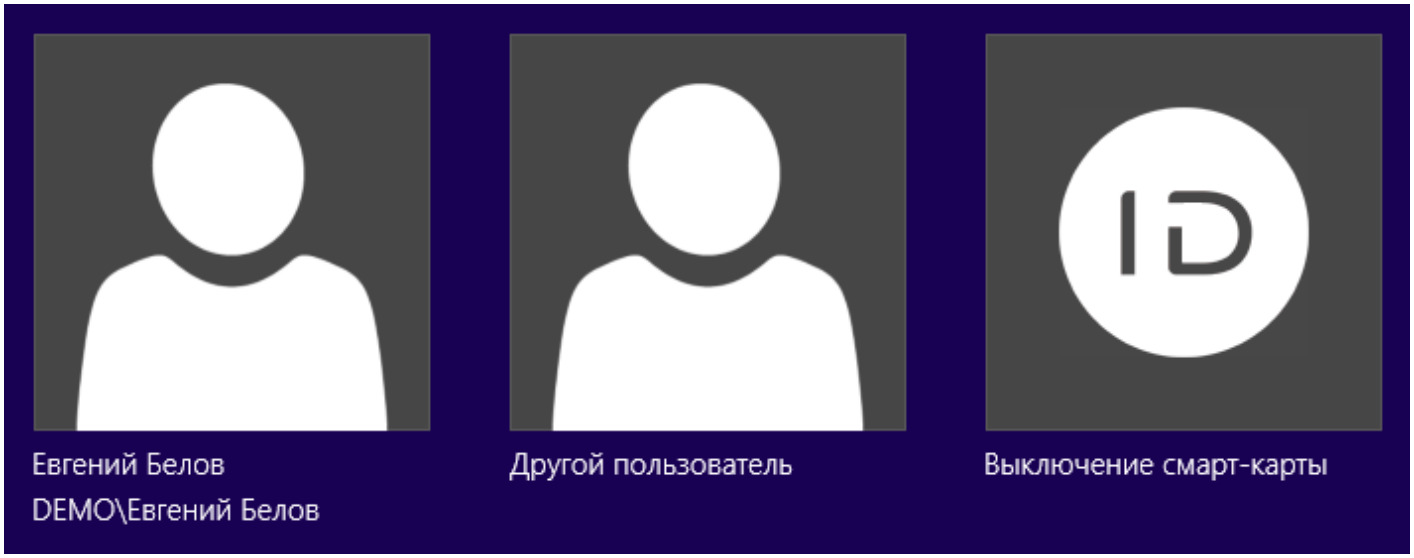

Рисунок 73 – Экстренное выключение устройства.

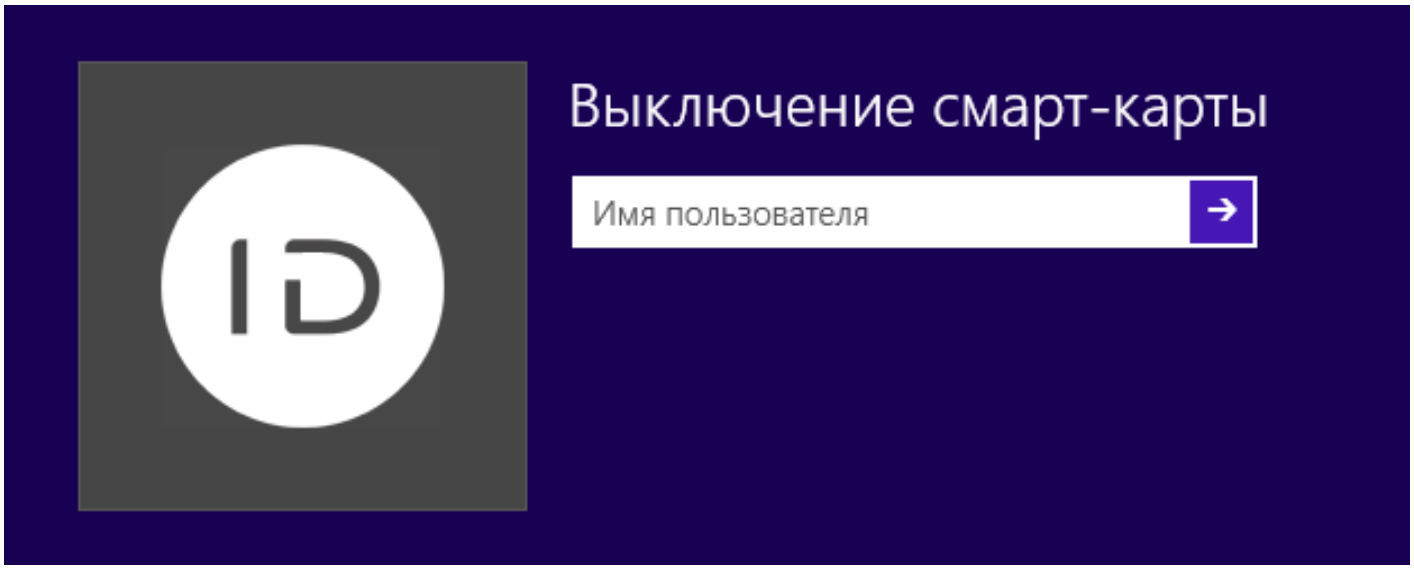

Рисунок 74 – Ввод имени пользователя для выключения устройства.

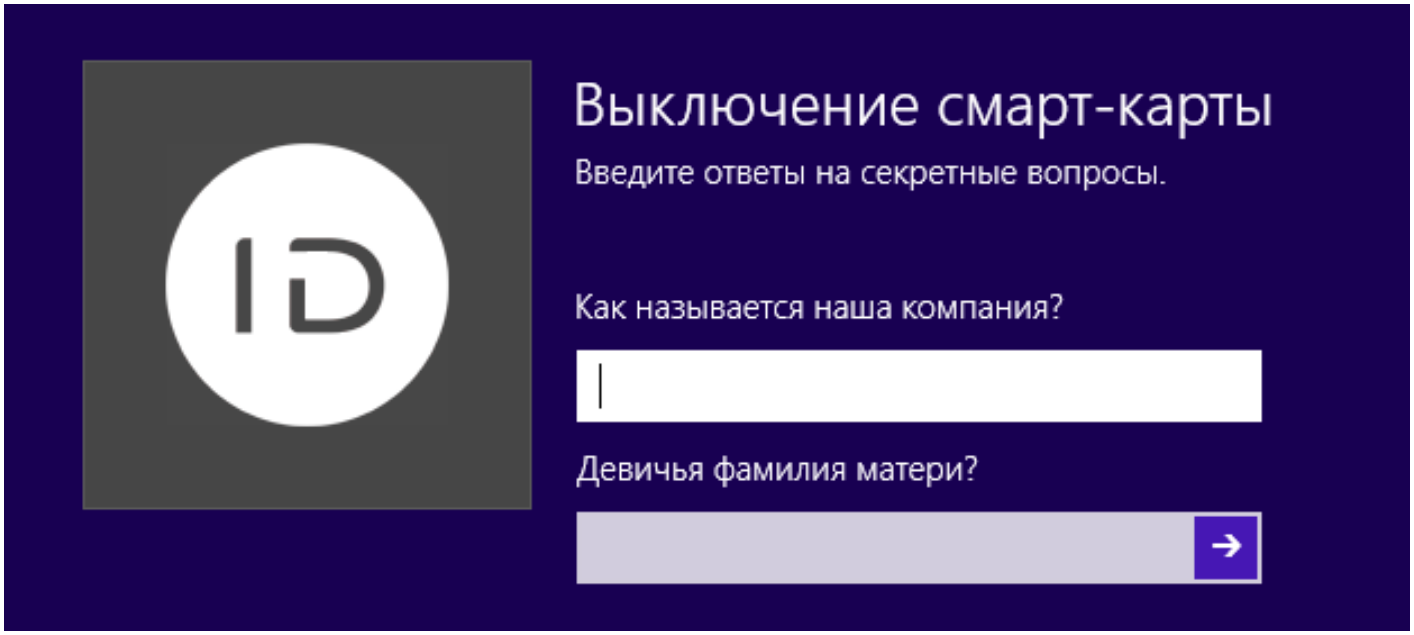

Рисунок 75 – Аутентификация пользователя по секретным вопросам.

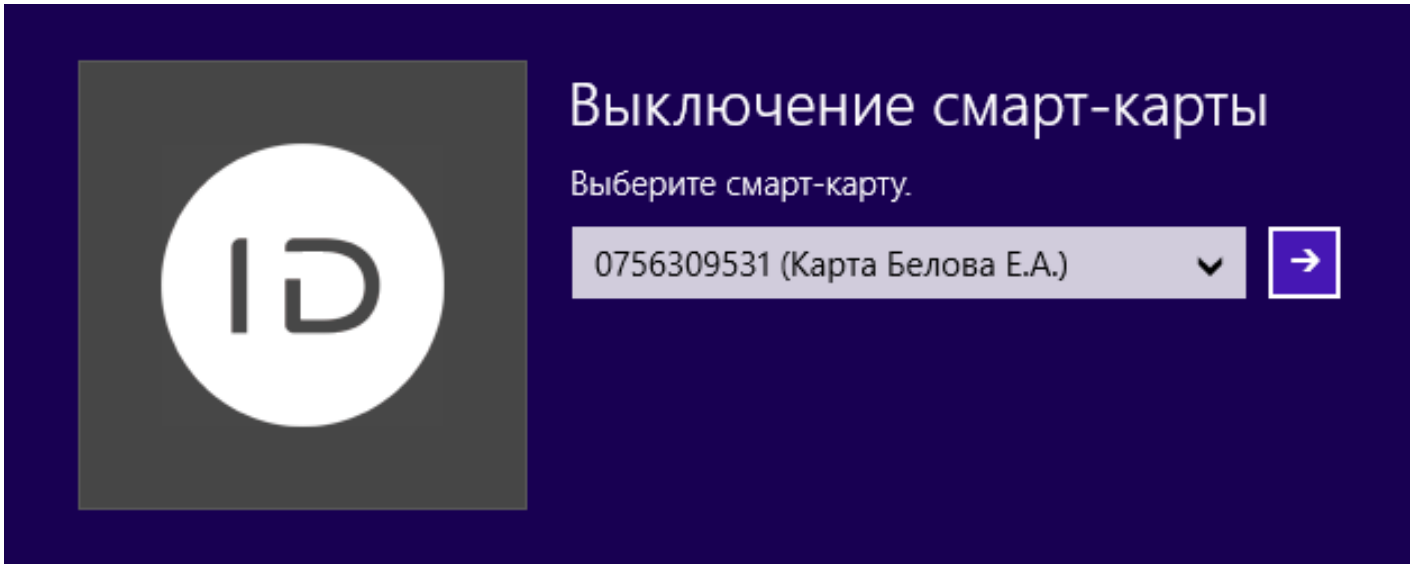

Рисунок 76 – Выбор устройства для выключения.

В случае успешного выключения устройства появится соответствующее сообщение.

Разблокировка пользователя. Помимо блокировки устройства пользователя в Indeed CM реализован и механизм блокировки учетной записи пользователя. Учетная запись пользователя блокируется в случае, если число неверных попыток ответов на секретные вопросы сравнялось с числом, заданным в параметрах политики использования устройств (параметр **Максимальное количество попыток аутентификации**) при попытке разблокировать устройство online или выполнить вход в приложение Remote Self Service.
В случае блокировки учетной записи пользователя, в журнал событий системы заносится соответствующая запись, а в карточке пользователя появляется соответствующий статус (Рисунок 77).

Заблокированный пользователь **не сможет использовать Remote Self Service и разблокировать/выключить устройство с использованием Indeed CM Credential Provider**.

Если заблокированы и устройство и пользователь, то оператор системы сможет разблокировать устройство, без разблокировки пользователя только в том случае, если в политике использования устройств отключена опция **Проверять ответы на секретные вопросы** в разделе **Поведение**.

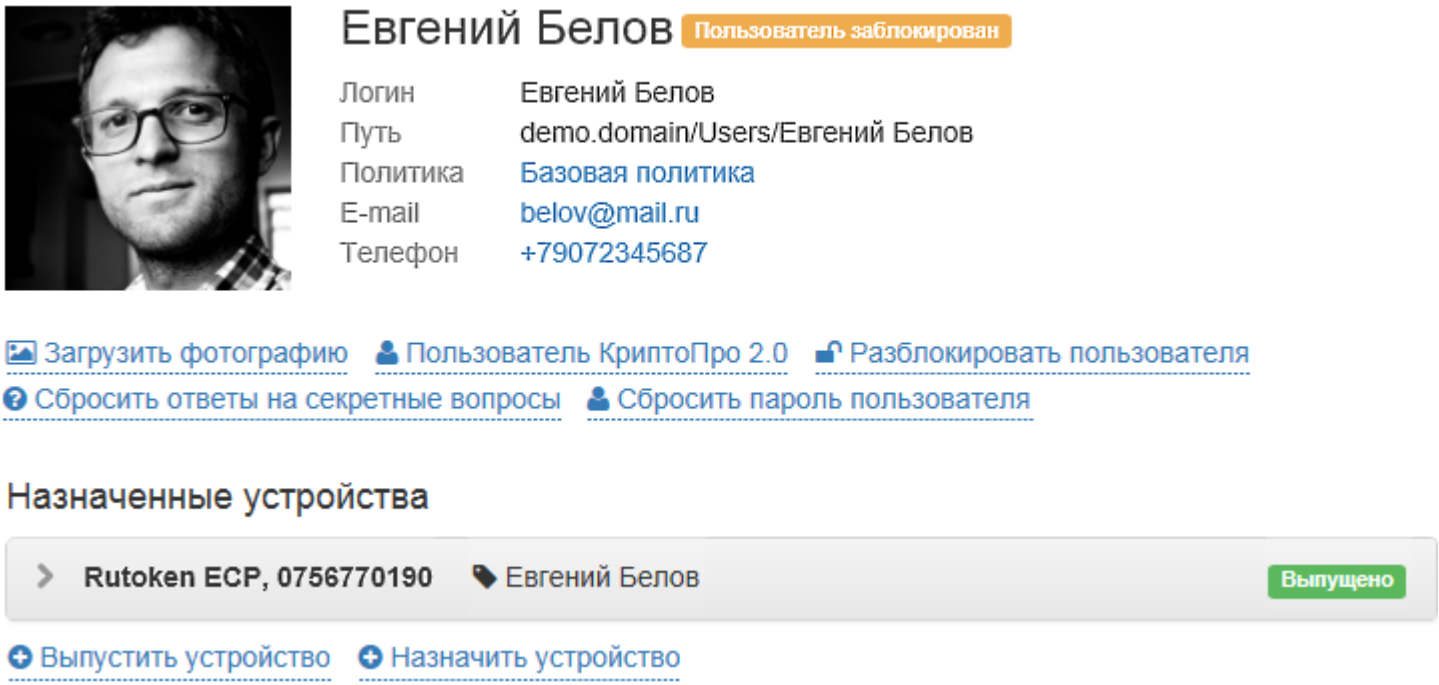

Рисунок 77 – Карточка заблокированного пользователя.

Для разблокировки пользователя нажмите **Разблокировать пользователя** и подтвердите действие нажатием кнопки **Разблокировать**.

Выключение и включение устройства. Устройство пользователя может быть выключено на определенный промежуток времени и затем снова включено. Например, на период отпуска сотрудника.
Для выключения устройства пользователя выполните следующие действия:

1. Перейдите на вкладку **Пользователи** и выполните поиск пользователя.
2. Перейдите в карточку пользователя, щелкнув по его логину в результатах поиска.
3. Выберите нужное устройство и раскройте информацию о нем.
4. Нажмите **Выключить**.

При попытке использования выключенного устройства для аутентификации пользователь получит сообщение о том, что его сертификаты отозваны. Для включения устройства пользователя выполните следующие действия:

При выключении устройства Indeed CM сможет отозвать все сертификаты, хранящиеся на нем. Для этого необходимо в политике использования устройств включить опцию **Отзывать сертификат при отзыве/выключении устройства**. Сертификаты будут отозваны с отметкой **Приостановка действия** (Certificate hold). Для возобновления действия сертификатов необходимо включить устройство.

Выключение и включение устройства оператором осуществляется без подключения устройства к рабочей станции.

1. Перейдите на вкладку **Пользователи** и выполните поиск пользователя.
2. Перейдите в карточку пользователя, щелкнув по его логину в результатах поиска.
3. Выберите нужное устройство и раскройте информацию о нем.
4. Нажмите **Включить**.

Отзыв устройства. Устройство может быть отозвано оператором (или пользователем, если определены соответствующие настройки в политике использования устройств) в случае его повреждения, утери, необходимости обновления или изъятия.

При включенной в политике использования устройств опции **Отзывать сертификат при отзыве/выключении устройства** все сертификаты пользователя, хранящиеся на устройстве, будут отозваны без возможности их восстановления.

Для отзыва устройства пользователя выполните следующие действия:

1. Перейдите на вкладку **Пользователи** и выполните поиск пользователя.
2. Перейдите в карточку пользователя, щелкнув по его логину в результатах поиска.
3. Выберите нужное устройство и раскройте информацию о нем.
4. Нажмите **Отозвать**.
5. Укажите причину отзыва:
   - Устройство неисправно
   - Устройство потеряно
   - Обновление устройства
   - Изъятие устройства
6. Нажмите кнопку **Отозвать**.

Причины отзыва устройства:

Устройство неисправно – устройство технически неисправно или уничтожено.

Устройство утеряно – устройство утеряно.

Обновление устройства – обновление устройства (например, замена старого устройства новым).

В случае, если устройство отзывается по причине того, что было утеряно, то все сертификаты, записанные на нем, будут отозваны (даже если не включена опция **Отзывать сертификат при отзыве/выключении устройства** в политике использования устройств.

Изъятие устройства – удаление устройства из системы в связи с увольнением сотрудника.

Причина отзыва устройства отображается в карточке пользователя. При попытке использования отозванного устройства для аутентификации пользователь получит сообщение о том, что его сертификаты отозваны.

Изъятие устройства. Отозванное устройство пользователя остается закрепленным за ним и может быть либо заменено (см. Замена устройства) либо изъято. Для изъятия устройства пользователя выполните следующие действия:

1. Перейдите на вкладку **Пользователи** и выполните поиск пользователя.
2. Перейдите в карточку пользователя, щелкнув по его логину в результатах поиска.
3. Выберите нужное устройство и раскройте информацию о нем.
4. Нажмите **Изъять** (Рисунок 78).
5. Если устройство доступно, выберите соответствующий пункт и подключите его к рабочей станции.
   - Если при выпуске устройства было создано СКЗИ, то необходимо указать номер документа, на основании которого происходит уничтожение СКЗИ в процессе изъятия.
   - Укажите PIN-код пользователя, который должен быть установлен на устройстве после его изъятия.

PIN-код необходимо устанавливать в том случае, если PIN-код пользователя, указанный в файле типа устройства (см. Управление типами устройств), не соответствует требованиям PIN-кода, установленным для данного типа устройства при инициализации в момент выпуска (см. Параметры инициализации устройства).

Если PIN-код пользователя не будет задан, то после изъятия устройства будет установлен PIN-код, указанный в файле типа устройства.

6. Подтвердите действие нажатием кнопки **Изъять**.
7. Если устройство недоступно, выберите соответствующий пункт и нажмите **Изъять**.

Замена устройства. Indeed CM позволяет выполнять временную или постоянную замену устройств пользователей. В этом случае содержимое одного устройства будет полностью перенесено на другое устройство.
Существует два типа замены устройства:

Временная замена – новое устройство будет выдано на определенный срок. Например, сотрудник забыл свою смарт-карту дома. Для работы в офисе оператор выпускает ему новую, срок действия

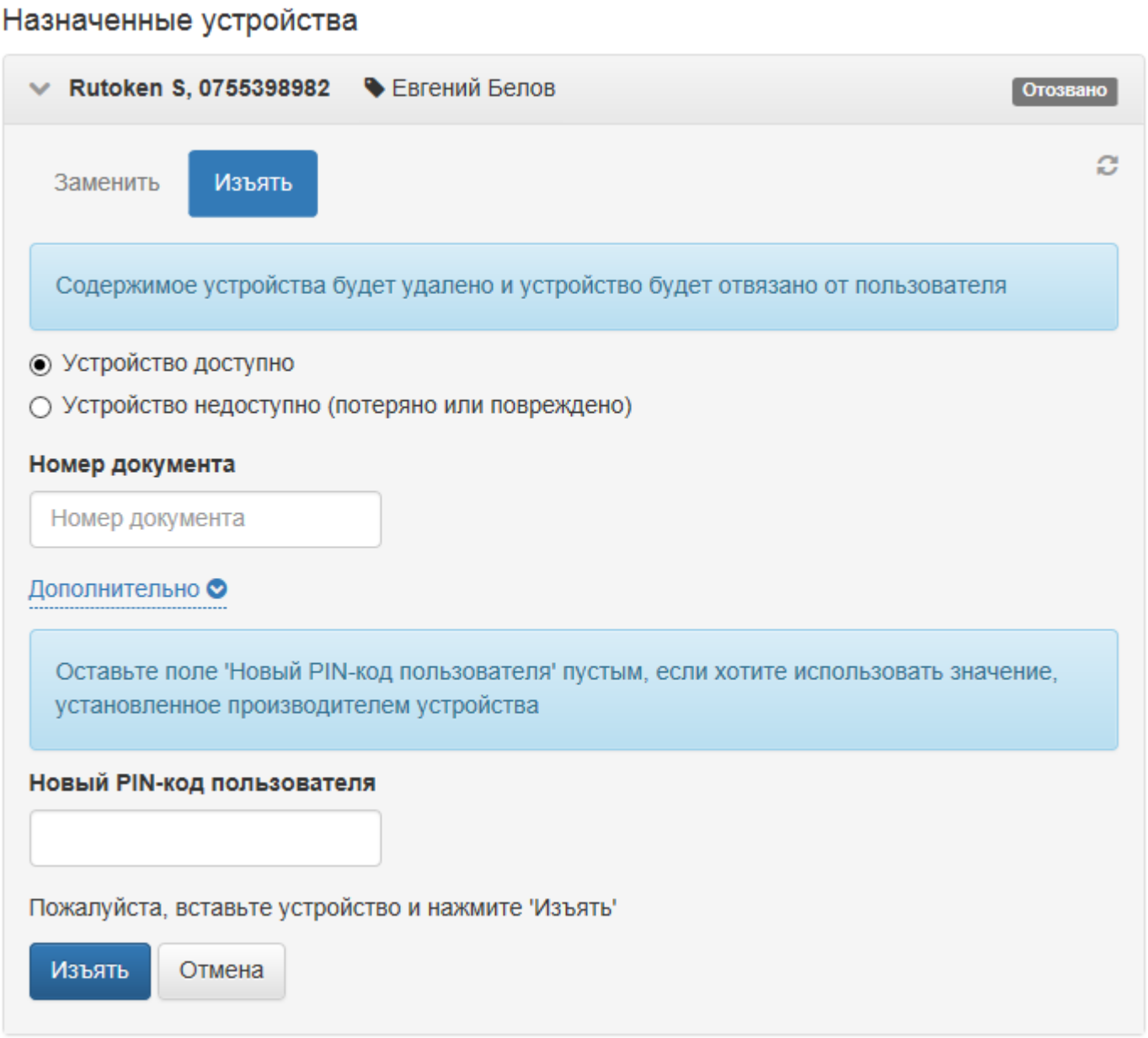

Рисунок 78 – Изъятие доступного устройства пользователя.

которой ограничен одними сутками.
В этом случае действие сертификатов на забытой дома карте сотрудника будет приостановлено. Действительные сертификаты и ключи будут записаны на новую смарт-карту (устройство). На Рисунке 79 в карточке пользователя отображаются два устройства:

- **Основное** устройство **Rutoken S** выключено и действие всех сертификатов, находящихся на нем приостановлено.
- **Устройство-дубликат Rutoken ECP** выпущено с ограниченным сроком действия (выделен красным).

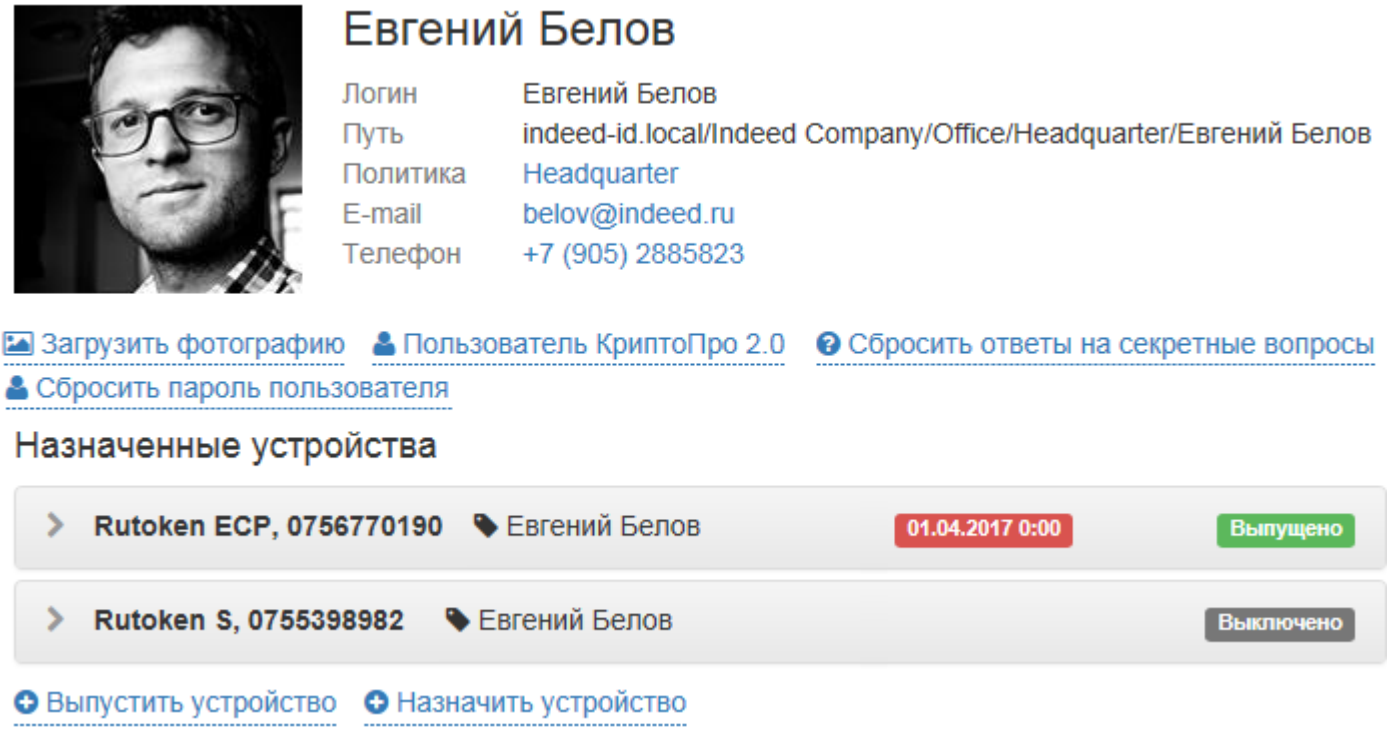

Рисунок 79 – Основное и временное устройства пользователя.

Постоянная замена – заменяемое устройство будет отозвано, вместо него будет выпущено новое. На новое устройство будут записаны все данные заменяемого устройства (ключевые пары, сертификаты). Сертификаты, хранящиеся на заменяемом устройстве, будут отозваны без возможности восстановления.

При замене устройства PIN-код устройства не переносится на новое устройство. Устройство-дубликат будет иметь PIN-код, в соответствии с настройками политики использования устройств:

- установленный производителем по умолчанию
- заданный администратором в параметрах инициализации устройства
- случайный

Изменить PIN-код устройства пользователь может в сервисе самообслуживания Self Service если определены соответствующие настройки в политике использования устройств.

Для замены устройства пользователя выполните следующие действия:

1. Перейдите на вкладку **Пользователи** и выполните поиск пользователя.
2. Перейдите в карточку пользователя, щелкнув по его логину в результатах поиска.
3. Выберите нужное устройство и раскройте информацию о нем.
4. Нажмите **Заменить**.
5. Укажите тип замены: **Временная** или **Постоянная**.
6. Если требуется временная замена, укажите срок окончания действия временной устройства.

7. Если требуется постоянная замена, укажите причину.
8. Задайте имя устройства (может быть подставлено автоматически, если в политике использования устройств разрешено соответствующее действие).
9. Подключите новое устройство к компьютеру.
10. Укажите PIN-код администратора в разделе **Дополнительно**, если новое устройство не добавлено в Indeed CM и нажмите **Заменить** (Рисунок 80) для замены устройства или **Отмена** для возврата к карточке пользователя.

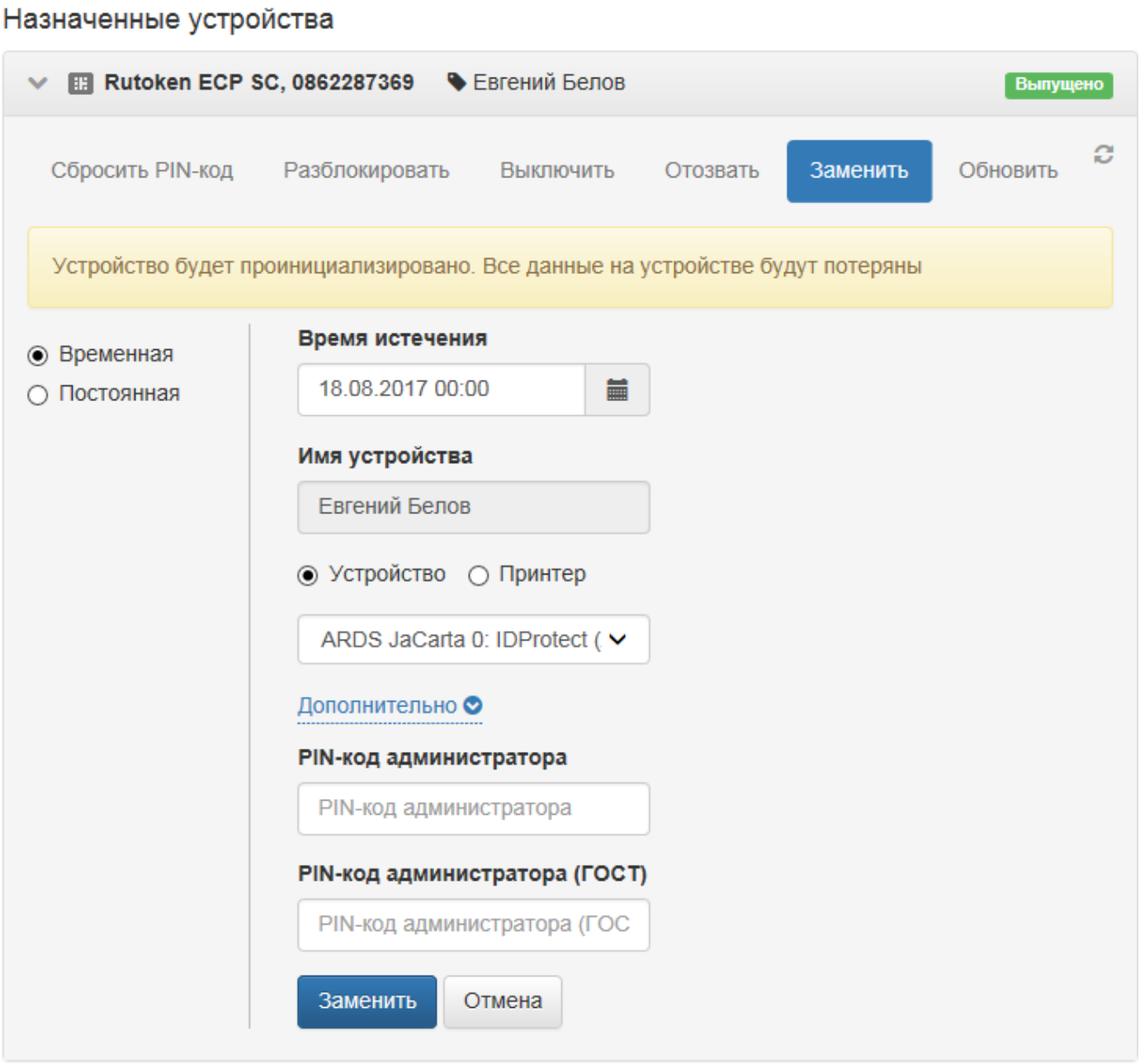

Рисунок 80 – Замена устройства.

Если Indeed Card Management интегрирован с Indeed AirKey Enterprise, то аппаратное устройство может быть заменено на виртуальную карту AirKey. Для замены на AirKey нажмите **Заменить на AirKey** в панели доступных действий с устройством.

Если определены соответствующие настройки в политике использования устройств, то в процессе замены новое устройство будет инициализировано. Все данные, хранящиеся на устройстве будут удалены.

Обновление устройства. Обновление устройства необходимо в случаях если:

- Срок действия одного или нескольких сертификатов пользователя истек (или истекает)
- В политике использования устройств изменилось количество шаблонов сертификатов
- В политике использования устройств присутствует хотя бы один необязательный сертификат (для последующей его записи или удаления на устройство/с устройства)
- В политике использования устройств включен или отключен коннектор к Indeed EA & ESSO
- Пользователю была назначена новая политика (например, с бóльшим приоритетом)

Если пользователю была назначена новая политика, то обновление содержимого устройства будет произведено следующим образом:

1. Сертификаты, которые есть в текущей политике, действующей на пользователя, но отсутствуют в новой, удалятся.
2. Сертификаты, которые есть в новой политике, но отсутствуют в текущей, будут выпущены и записаны на устройство.
3. Сертификаты, присутствующие в обеих политиках, останутся без изменений.

Администратор может обновить содержимое устройства без его перевыпуска. Обновление содержимого устройства по умолчанию также доступно и пользователю в приложении Self Service.

Для обновления устройства выполните следующие действия:

1. Перейдите на вкладку **Пользователи** и выполните поиск пользователя.
2. Перейдите в карточку пользователя, щелкнув по его логину в результатах поиска.
3. Выберите нужное устройство и раскройте информацию о нем.
4. Нажмите **Обновить**.
5. Подключите устройство к компьютеру, введите PIN-код пользователя и нажмите **Обновить**.

Выпуск устройства с печатью. Если опция **Включить печать устройства** в политике использования устройств включена, то выпуск устройств в форм факторе смарт-карты в Indeed CM может быть объединен с печатью изображения или текста на них. В этом случае смарт-карта помещается в лоток подачи карт принтера и в процессе выпуска на неё записываются сертификаты и наносится изображение в соответствии с заданным шаблоном печати.

[25]Поставляется производителем вместе с принтером.
[26]Поставляется производителем вместе с принтером.
[27]Поставляется в составе дистрибутива Indeed CM.

Обязательным условием печати на устройствах является наличие на рабочей станции, с которой происходит печать следующих компонентов:

- Драйвера принтера EDISecure XID8300[25]
- Настроенного соединения с принтером в утилите EDI Secure Connect[26]
- Компонента поддержки принтера IndeedCM.EdiSecure.Middleware[27]
- Подключенного через интерфейс USB принтера XID8300

Для выпуска смарт-карты с печатью выполните следующие действия:

1. Перейдите на вкладку **Пользователи** и выполните поиск пользователя.
2. Перейдите в карточку пользователя, щелкнув по его логину в результатах поиска.
3. Нажмите **Выпустить устройство**.
4. Укажите **Имя устройства**[28].
5. Если политика использования устройств подразумевает выбор сертификатов, выберите нужные и нажмите **Далее**.
6. Укажите способ выпуска устройства **Принтер**. Имя подключенного принтера подставится автоматически (Рисунок 81).

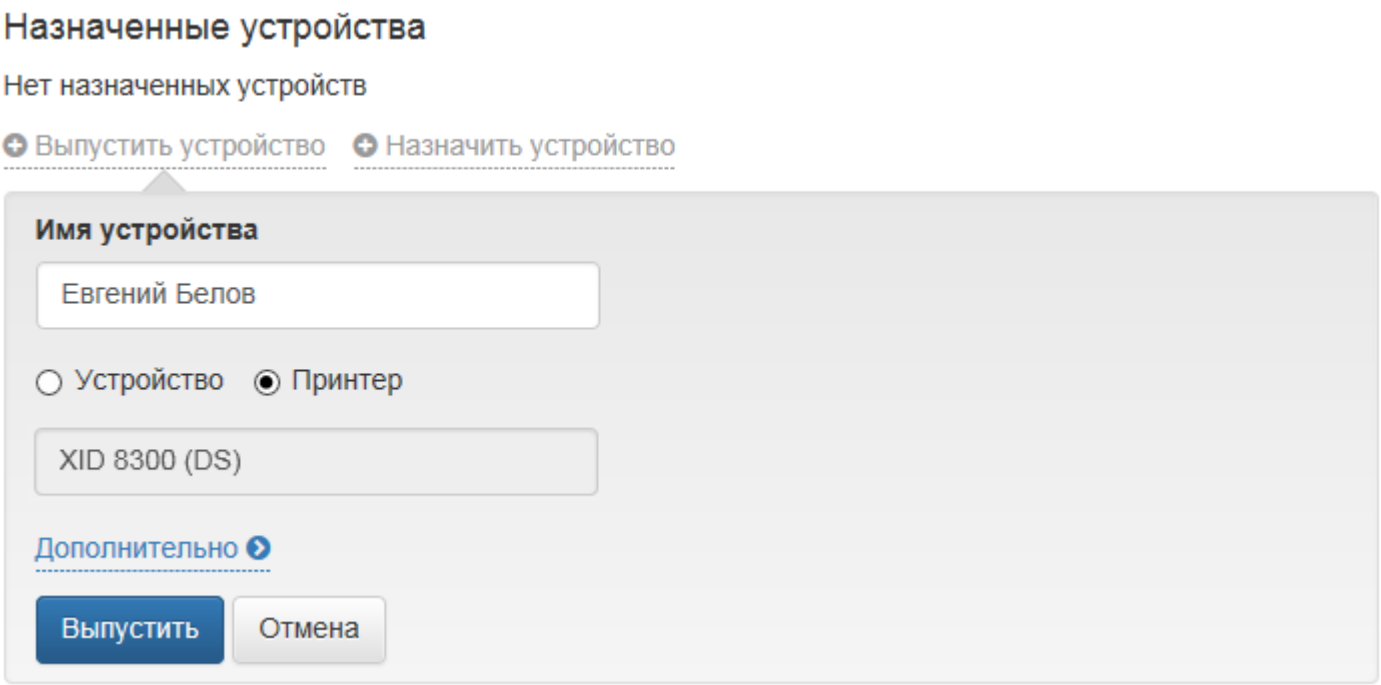

Рисунок 81 – Выпуск устройства с печатью.

7. Поместите карту в лоток подачи принтера.
8. Нажмите **Выпустить**.

[28]Имя устройства может быть подставлено автоматически. См. **Настройки выпуска устройства**.

Кроме того, система позволяет наносить изображение на ранее выпущенные (без использования принтера) карты.
Для печати на ранее выпущенной карте выполните следующие действия:

1. Поместите карту в лоток принтера.
2. Перейдите на вкладку **Пользователи** и выполните поиск пользователя.
3. Перейдите в карточку пользователя, щелкнув по его логину в результатах поиска.
4. Выберите нужную карту и раскройте информацию о ней.
5. Нажмите **Печатать**.

Массовый выпуск смарт-карт. При использовании Indeed CM с принтером смарт-карт (опция **Включить поддержку принтера смарт-карт** в политике использования устройств) существует возможность массового выпуска карт пользователям. В этом случае оператор определяет группу пользователей, которым необходимо выпустить карты, помещает нужное количество карт в лоток принтера и запускает процесс массового выпуска.

Режим массового выпуска имеет следующие особенности и ограничения:

- Отсутствует возможность выбора необязательных сертификатов. Будут выпущены только обязательные. Необязательные сертификаты, в случае необходимости, следует выпустить для каждого пользователя отдельно через карточку пользователя или сервис самообслуживания.
- Отсутствует возможность указания имя карты. Имя будет пустым или сформированным по правилам, обозначенным в политике использования устройств.
- Отсутствует возможность создать автоматически документ учета СКЗИ. В случае необходимости, такой документ следует указать вручную в карточке пользователя.
- При возникновении любой ошибки массовый выпуск останавливается. Для дальнейшей работы следует устранить ошибку или исключить проблемного пользователя из списка и запустить массовый выпуск заново.
- При нажатии кнопки **Отмена** во время массового выпуска загруженная в принтер карта будет выпущена, выпуск следующей карты не будет начат.
- Массовый выпуск может осуществляться как с печатью данных на карте, так и без.

Обязательным условием массового выпуска является наличие на рабочей станции, с которой происходит печать следующих компонентов:

- Драйвера принтера EDISecure XID8300[29]
- Настроенного соединения с принтером в утилите EDI Secure Connect[30]
- Компонента поддержки принтера IndeedCM.EdiSecure.Middleware[31]
- Подключенного через интерфейс USB принтера XID8300

[29]Поставляется производителем вместе с принтером.
[30]Поставляется производителем вместе с принтером.
[31]Поставляется в составе дистрибутива Indeed CM.

Для массового выпуска устройств выполните следующие действия:

1. Перейдите на страницу сервиса *https://<адрес сервера Indeed CM >/icm/bulkissue*
2. Выполните поиск пользователей (например, по месту расположения). Результат поиска отобразится в таблице слева.
3. Отметьте среди найденных пользователей всех, кому необходимо выпустить смарт-карты и нажмите >.
4. Нажмите **Выпустить**. Имя будет подставлено автоматически (Рисунок 82).
5. Нажмите **Выпустить**.

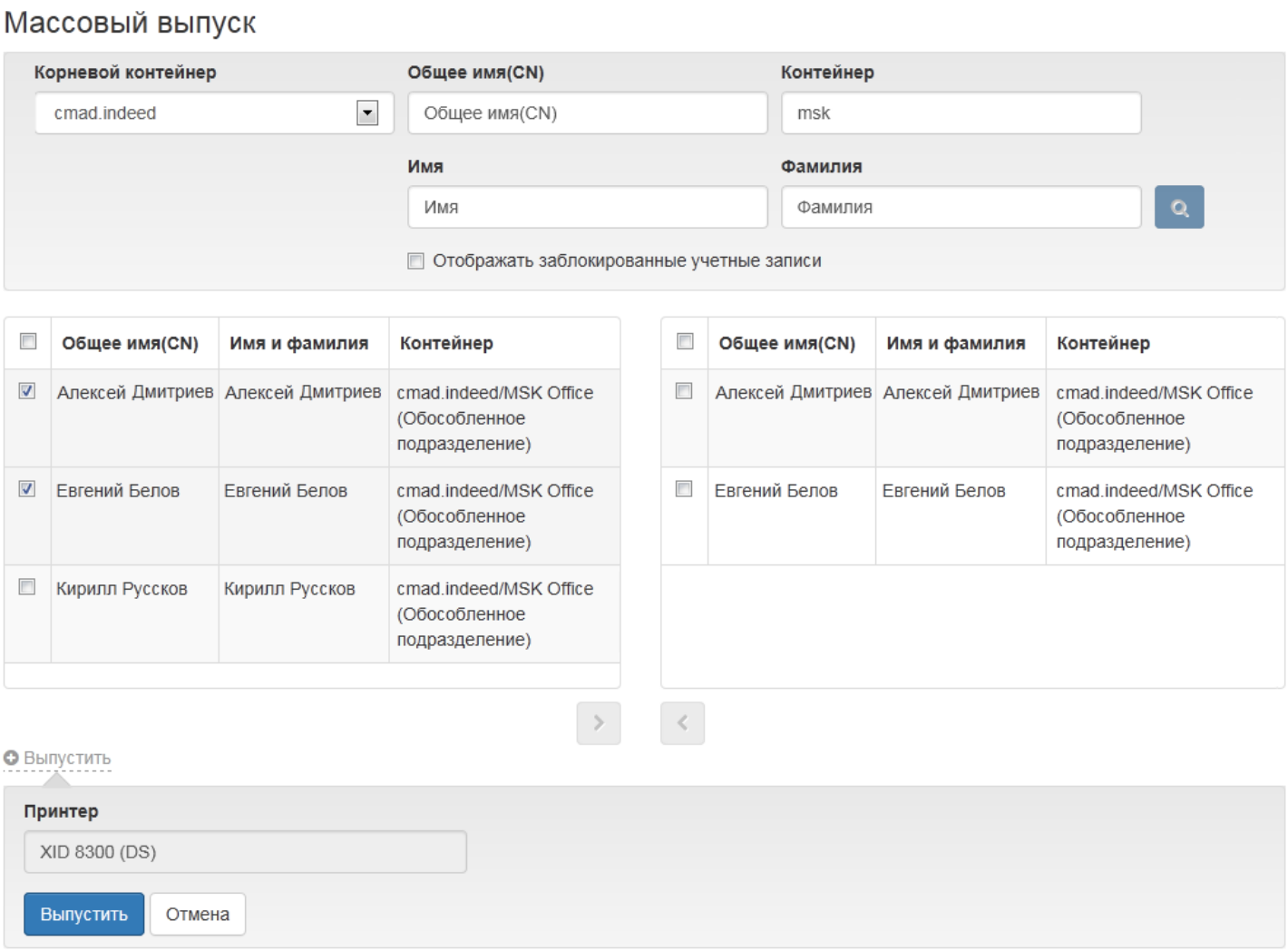

Рисунок 82 – Массовый выпуск смарт-карт.

Прогресс выпуска карты для каждого пользователя отображается в нижней части экрана (Рисунок 83). Выпуск карты можно приостановить нажав **Пауза** или отменить, нажав **Отмена**.

В случае возникновения ошибки при массовом выпуске, пользователь, на котором произошла ошибка, выделяется красным, а в нижней части экрана отображается текст ошибки (Рисунок 84).

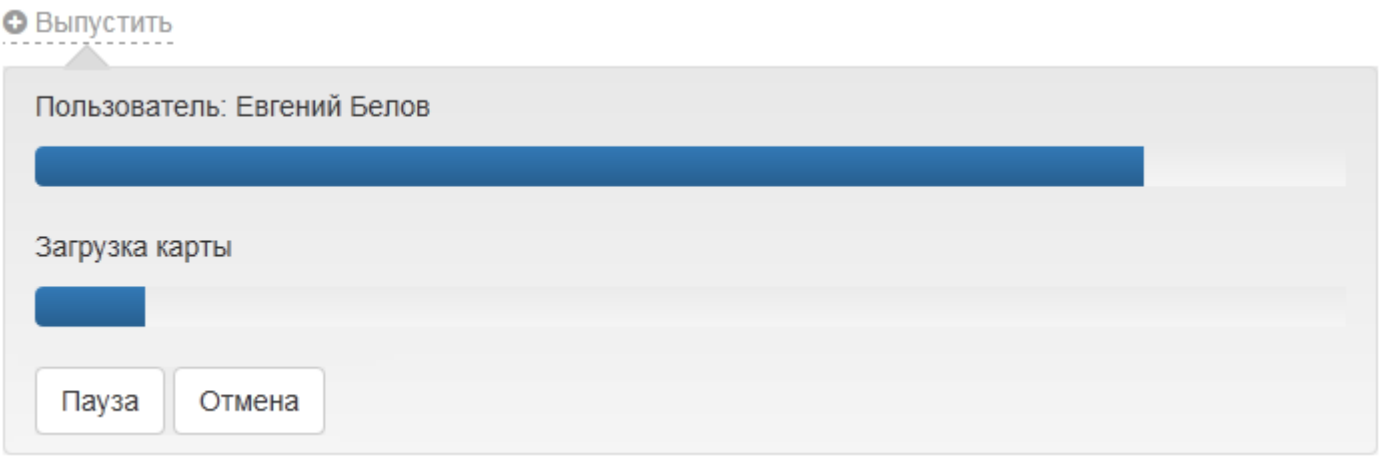

Рисунок 83 – Прогресс массового выпуска смарт-карт.

После устранения ошибки выпуск можно повторить нажав на соответствующую кнопку. Для игнорирования ошибки и продолжения массового выпуска карт нажмите **Пропустить**. Для отмены массового выпуска для всех пользователей нажмите **Отмена**.

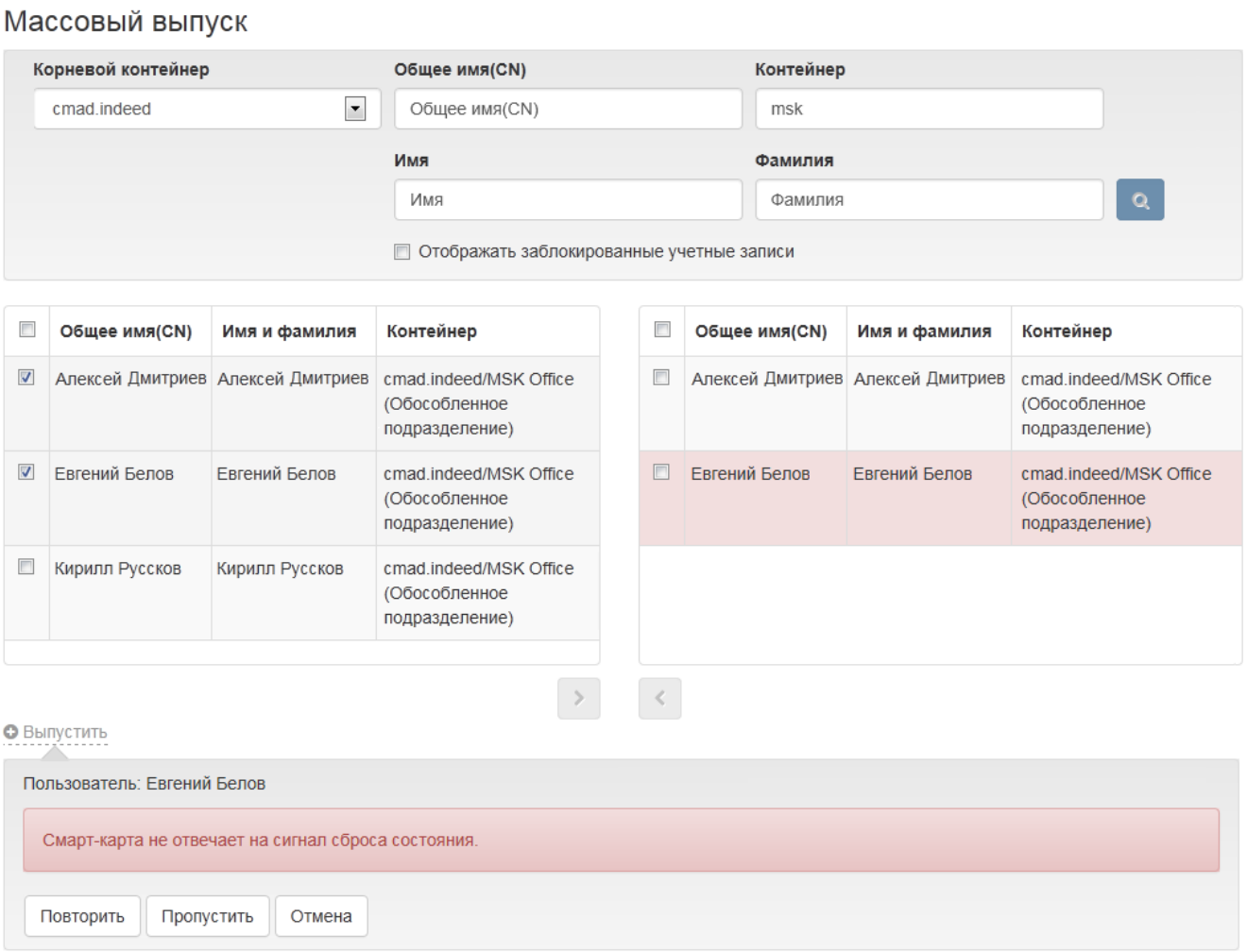

Рисунок 84 – Ошибка при массовом выпуске устройств.

Назначенные СКЗИ. Закрепленные за пользователем СКЗИ отображаются в его карточке (Рисунок 85). СКЗИ может быть добавлено при выпуске устройства пользователю (см. Выпуск устройства), или в любой другой момент времени.

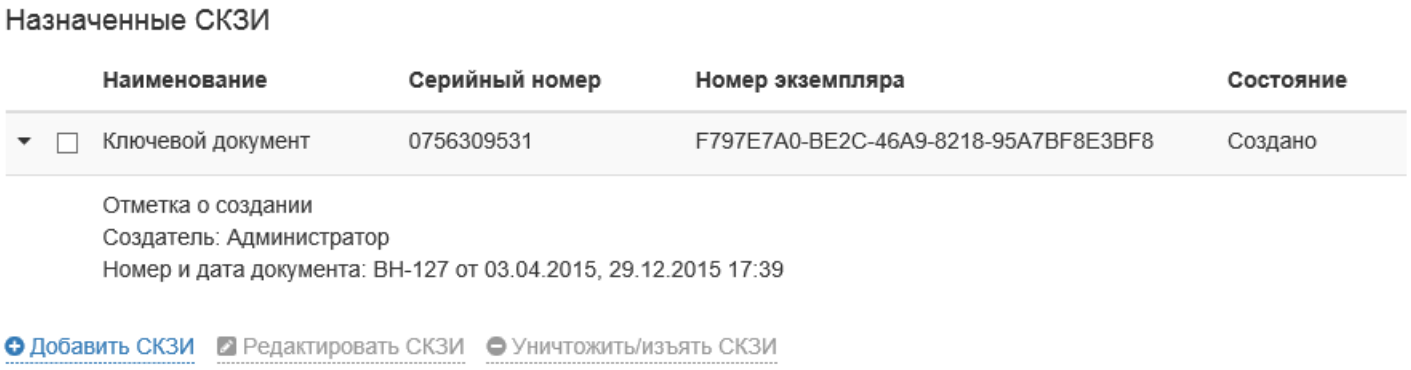

Рисунок 85 – Назначенные пользователю СКЗИ.

Нажмите **Добавить СКЗИ** для закрепления нового средства криптографической защиты за пользователем. Задайте значения параметров СКЗИ и нажмите **Добавить** (Рисунок 86):

- **Тип** (Дистрибутив, Лицензия, Документация, Ключевой документ, Пользовательский). Обязательно для заполнения.
- **Серийный номер**. Обязательно для заполнения.
- **Номер и дата документа**. Обязательно для заполнения.
- **Номер экземпляра**. При создании СКЗИ в момент выпуска устройства, устанавливается автоматически имя контейнера, содержащего ключевую пару. Необязательное поле для заполнения.

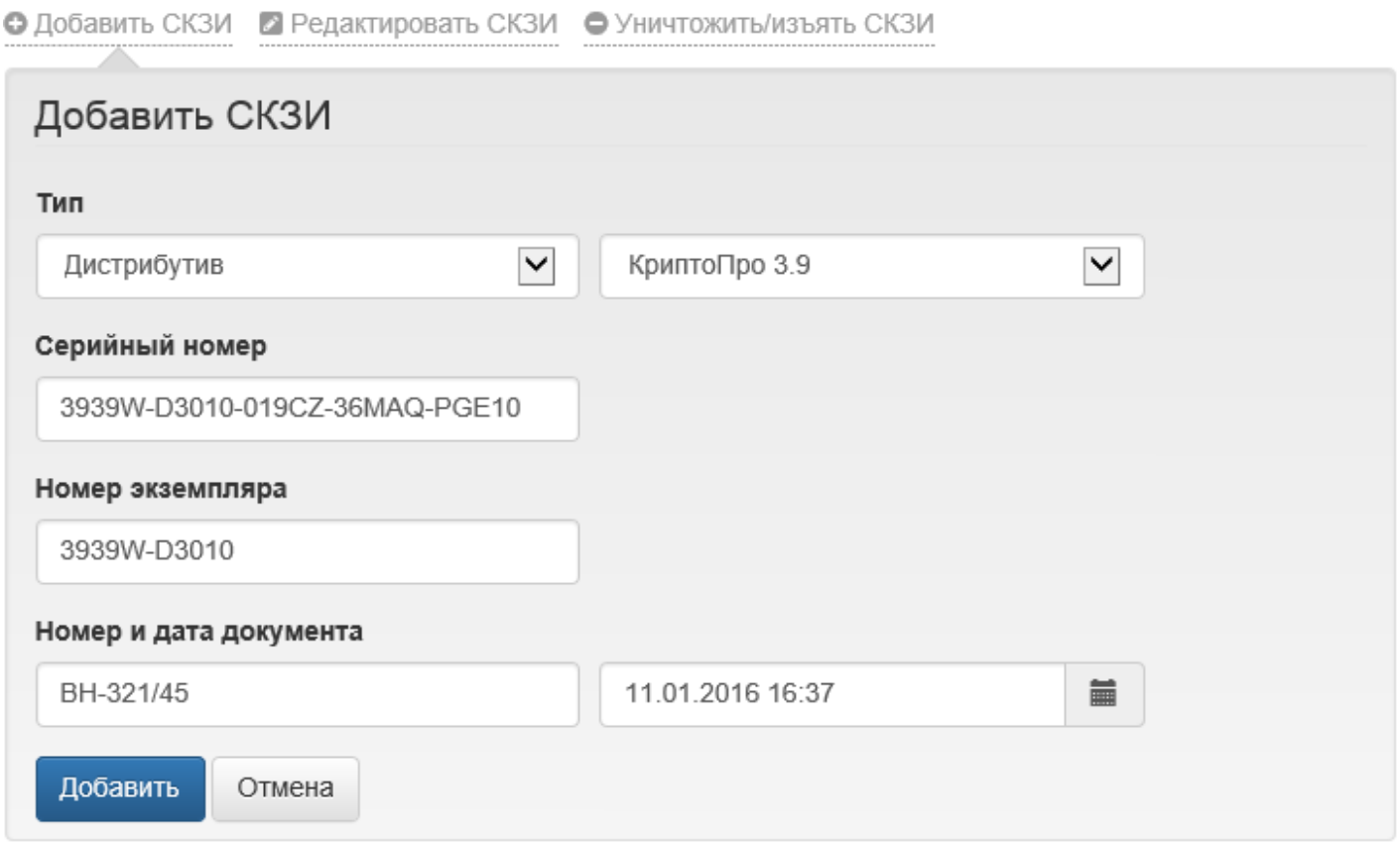

Рисунок 86 – Добавление СКЗИ.

Имеющиеся у пользователя СКЗИ могут быть отредактированы уполномоченным сотрудником (оператором или администратором Indeed CM). Для редактирования выберите средство криптографической защиты и нажмите **Редактировать СКЗИ** (Рисунок 87).

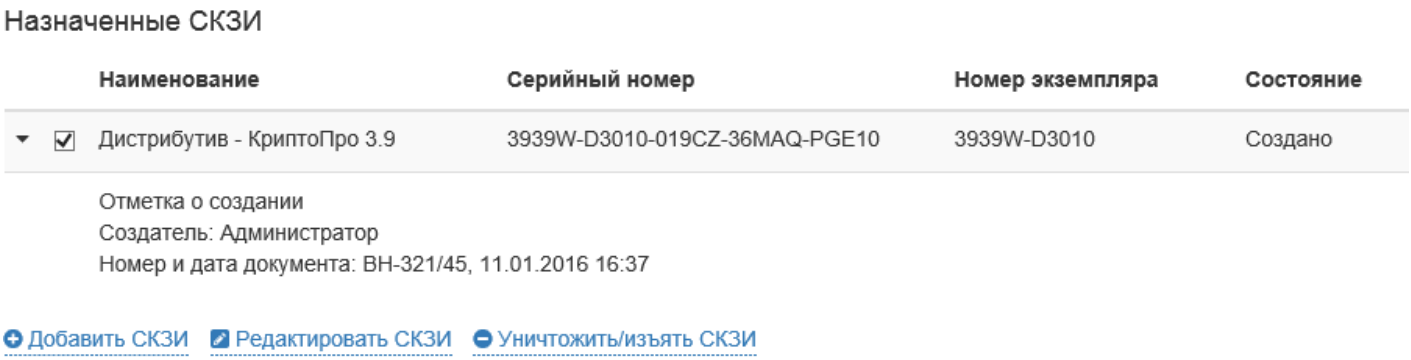

Рисунок 87 – Редактирование СКЗИ.

Ниже приведены поля, доступные для редактирования[32]:

- Отметка о передаче
- Отметка о возврате
- Отметка о выдаче
- Отметка о подключении
- Примечание

Внесите необходимые изменения и нажмите **Сохранить**.

Для изъятия СКЗИ выберите средство криптографической защиты и нажмите **Уничтожить/изъять СКЗИ**. Укажите имя сотрудника, выполняющего изъятие СКЗИ, номер и дату документа, на основании которого осуществляется изъятие/уничтожение и нажмите **Уничтожить** (Рисунок 88).

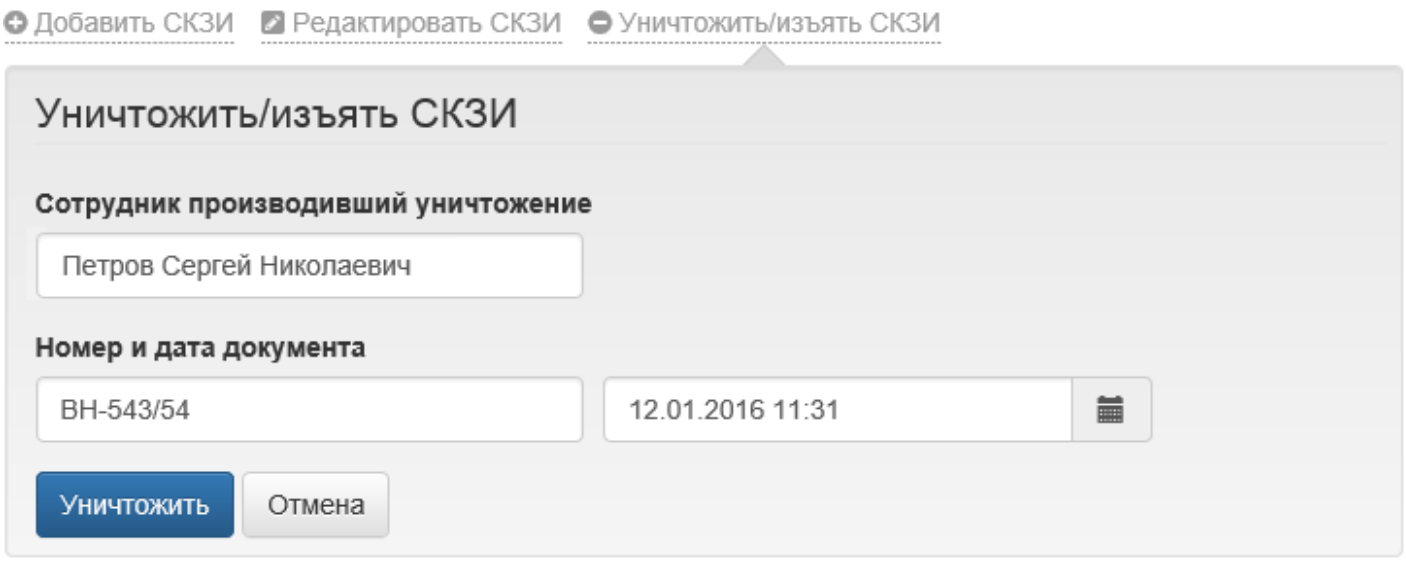

Рисунок 88 – Уничтожение СКЗИ.

События пользователя. В карточке пользователя отображается информация о пяти последних событиях в системе Indeed CM для этого пользователя. Список событий можно обновить нажав кнопку ↻. Чтобы посмотреть информацию по нужному событию, нажмите ▶ (Рисунок 89).

[32]Перечень полей указан в соответствии с типовой формой журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (для органа криптографической защиты), утвержденной Приказом ФАПСИ от 13 июня 2001 г. №152.

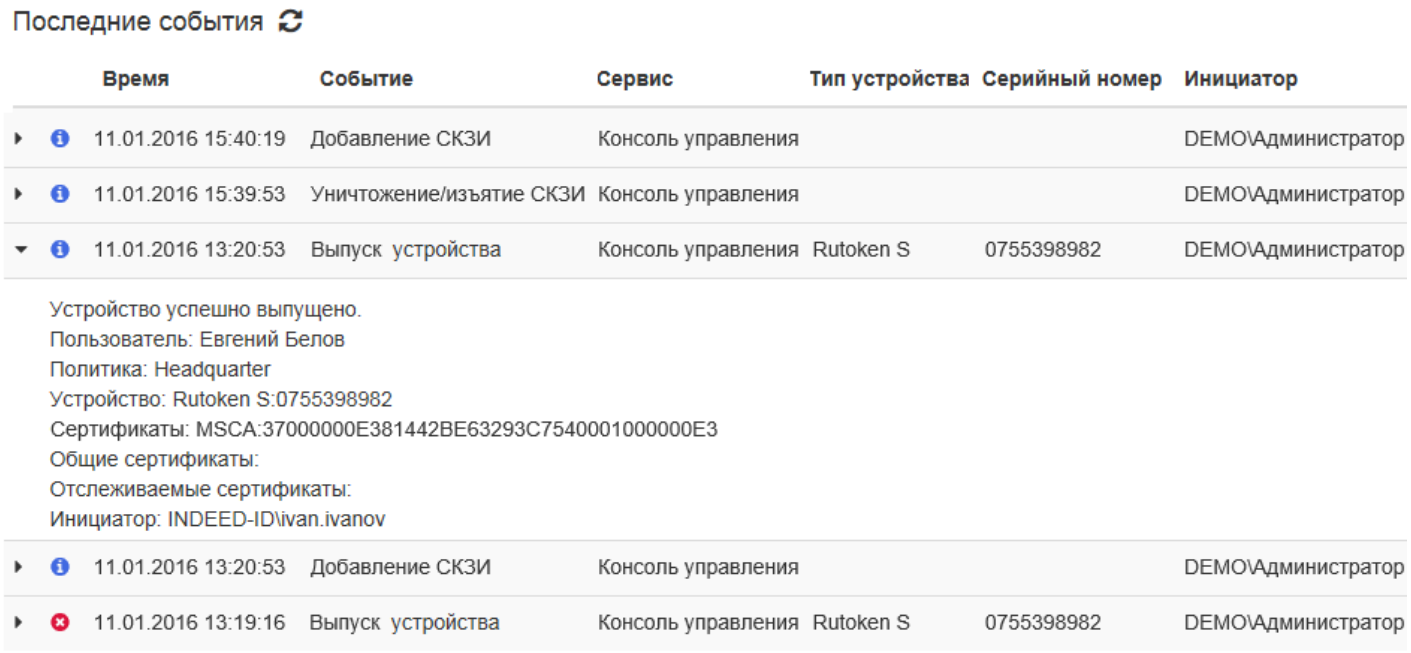

Рисунок 89 – Последние 5 событий пользователя.

Для просмотра полного списка событий и перехода в раздел **Журнал** нажмите **Просмотреть все**.

СКЗИ

Раздел для работы со средствами криптографической защиты информации.

Добавление и редактирование СКЗИ

Добавление и редактирование СКЗИ аналогичны таковым в Карточке пользователя.

Для поиска СКЗИ установите параметры выборки:

- **Тип** (Не задано, Дистрибутив, Лицензия, Документация, Ключевой документ, Пользовательский)
- **Подтип** (Не задано, Неустановленный, КриптоПро 3.6, КриптоПро 3.9, КриптоПро 4.0,)
- **Пользователь**
- **Серийный номер**
- **Номер экземпляра**
- **Состояние** (Создано, Передано, Возвращено, Выдано, Установлено, Уничтожено)
- **Период времени поиска**

Пример вывода результатов поиска СКЗИ за указанный период времени приведен на Рисунке 90. Результаты поиска СКЗИ могут быть сохранены в виде файла. Для создания файла нажмите и выберите формат.

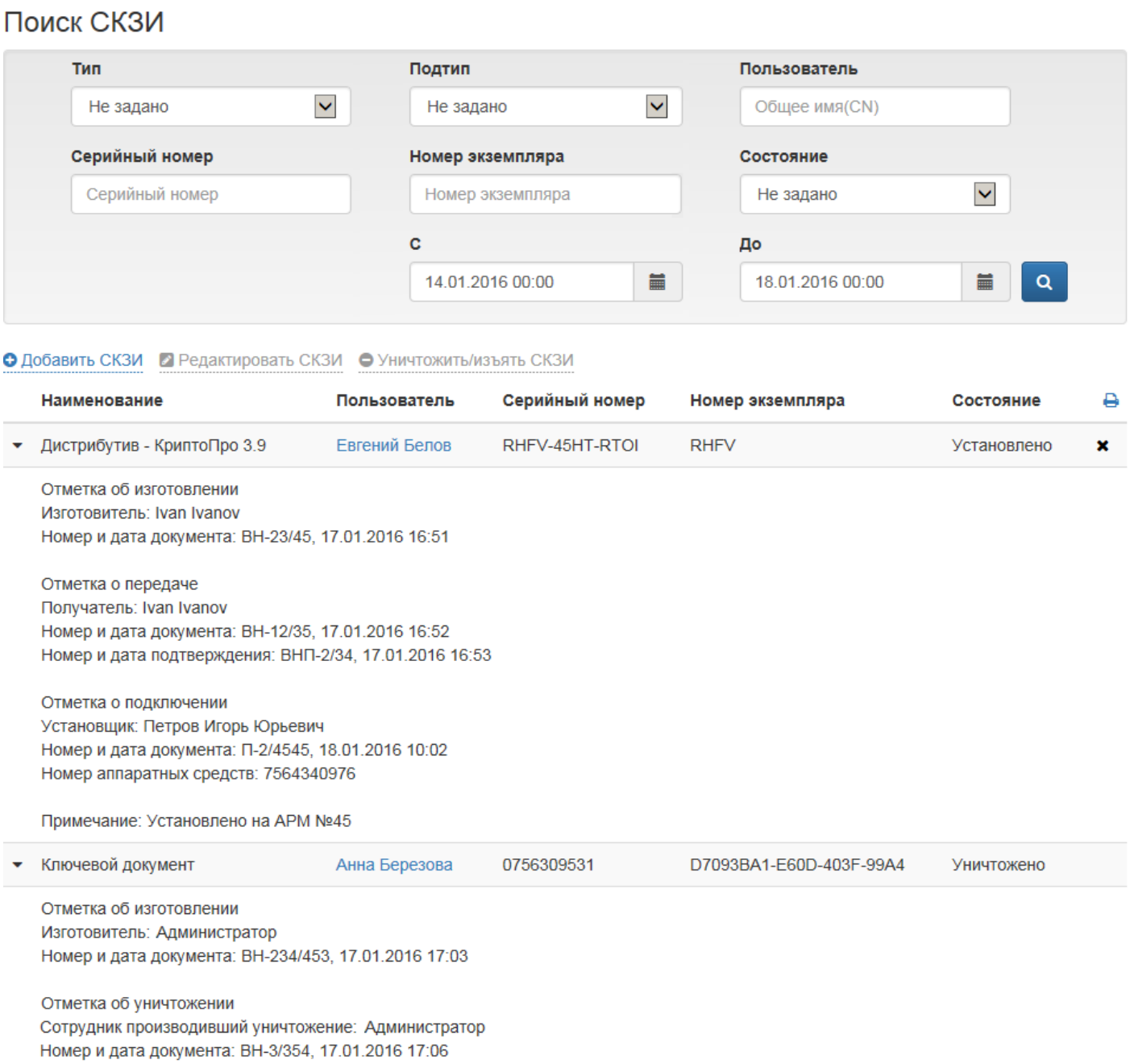

Рисунок 90 – Результат поиска СКЗИ.

Сохраните полученный файл. Пример PDF файла с результатами поиска приведен на Рисунке 91.

СКЗИ

Параметры поиска
С: 11.01.2016 0:00
До: 19.01.2016 0:00

Результат

N	Наименование	Пользователь	Серийный номер	Номер экземпляра	Состояние
1	Дистрибутив - КриптоПро 3.9	Евгений Белов	RHFV-45HT-RTOI	RHFV	Установлено
Отметка об изготовлении Изготовитель: Ivan Ivanov Номер и дата документа: ВН-23/45, 17.01.2016 16:51 Отметка о передаче Получатель: Ivan Ivanov Номер и дата документа: ВН-12/35, 17.01.2016 16:52 Номер и дата подтверждения: ВНП-2/34, 17.01.2016 16:53 Отметка о подключении Установщик: Петров Игорь Юрьевич Номер и дата документа: П-2/4545, 18.01.2016 10:02 Номер аппаратных средств: 7564340976 Примечание: Установлено на АРМ №45					
2	Ключевой документ	Анна Березова	0756309531	D7093BA1-E60D-403F-99A4	Уничтожено
Отметка об изготовлении Изготовитель: Ivan Ivanov Номер и дата документа: ВН-234/453, 17.01.2016 17:03 Отметка об уничтожении Сотрудник производивший уничтожение: Ivan Ivanov Номер и дата документа: ВН-3/354, 17.01.2016 17:06					

Рисунок 91 – Результат поиска СКЗИ в формате PDF.

Удаление СКЗИ

Для удаления СКЗИ нажмите ✖ . Укажите имя сотрудника, осуществляющего уничтожение, номер документа, на основании которого уничтожается СКЗИ и нажмите **Уничтожить** (Рисунок 92).

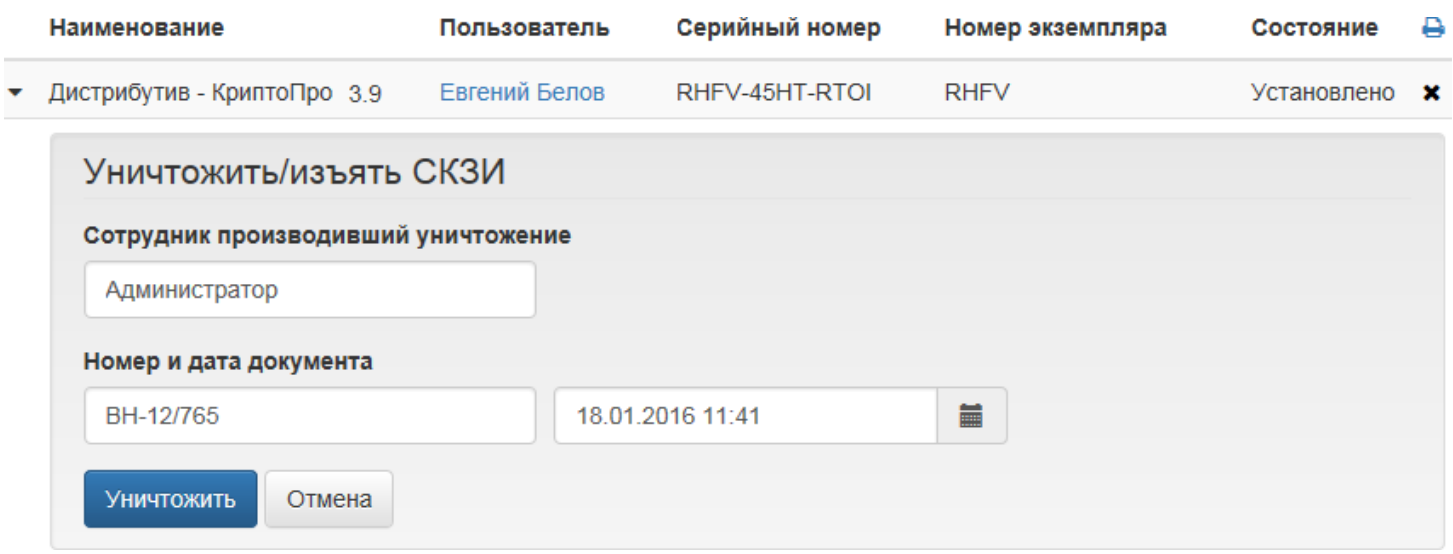

Рисунок 92 – Удаление СКЗИ.

Журнал

Записи о всех операциях во всех приложениях Indeed CM отражаются в журнале событий Indeed CM/Operational на сервере Indeed CM. В разделе **Журнал** администратор или оператор могут запрашивать необходимую информацию при помощи фильтров (Рисунок 93).

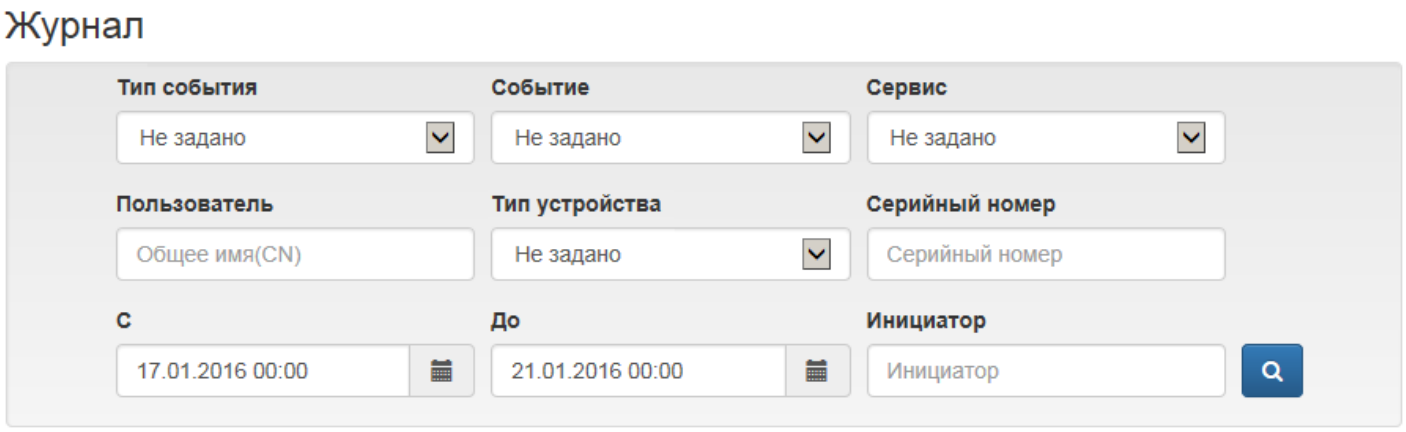

Рисунок 93 – Фильтры событий системы Indeed CM.

Indeed CM ведет учет событий следующих типов (Рисунок 94):

- **Информация** – успешное выполнение любой операции
- **Ошибка** – завершение любой операции с ошибкой
- **Предупреждение** – события, требующие внимания администратора системы

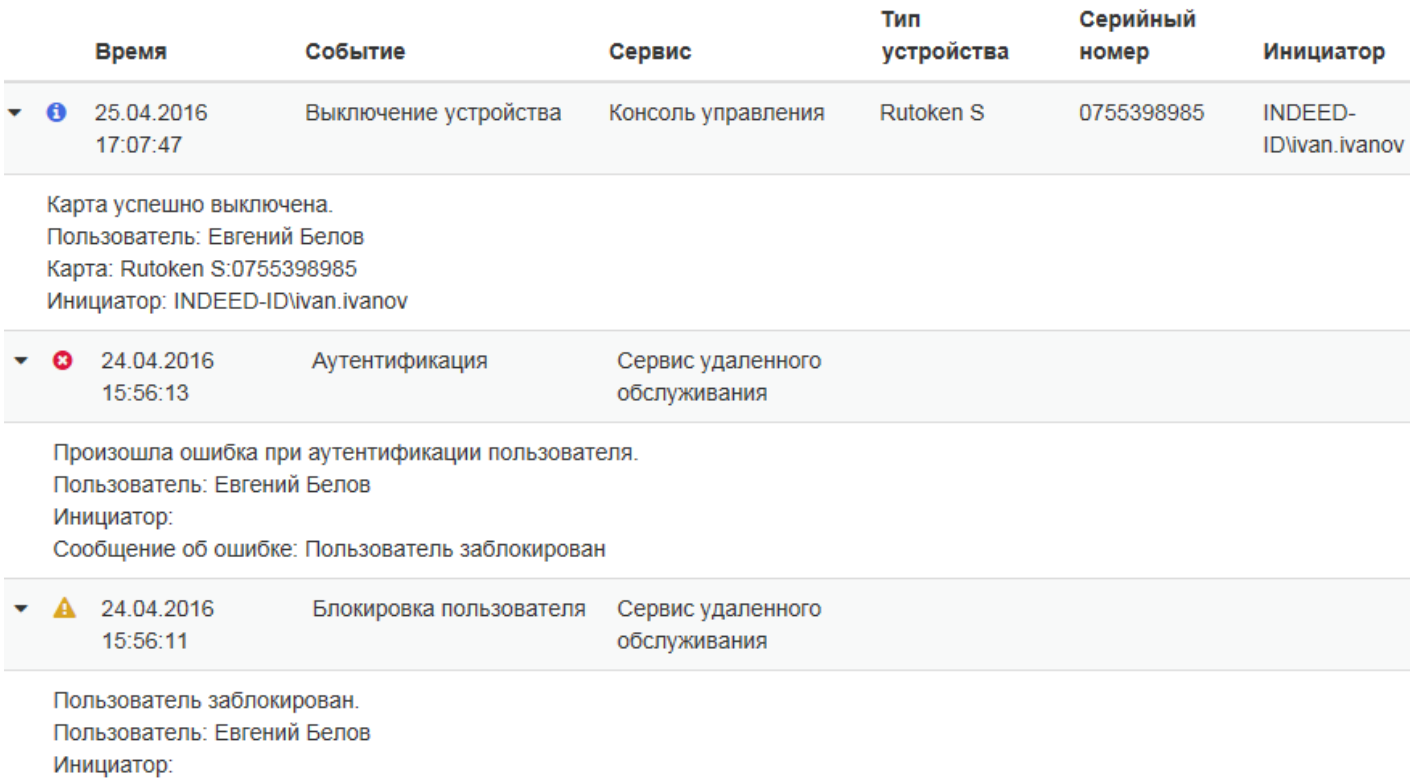

Рисунок 94 – Типы событий системы Indeed CM.

Для формирования отчета о событиях нажмите  и выберите формат. На Рисунке 95 отображаются последние события, а на Рисунке 96 отчет по этим событиям в формате PDF. Полный список событий приведен в разделе Список событий Indeed CM.

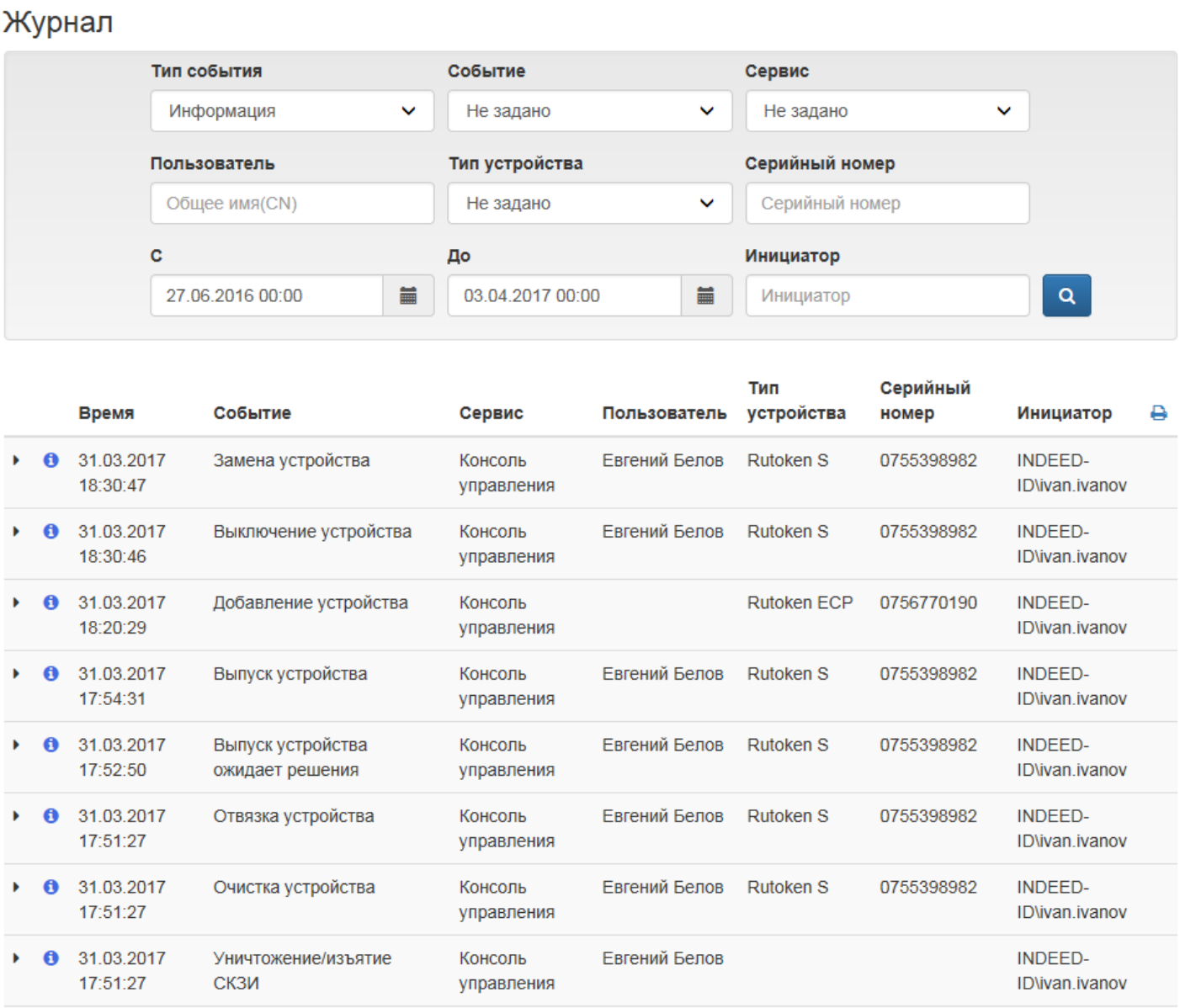

Рисунок 95 – Журнал событий системы Indeed CM.

События

Параметры поиска

Тип события: Информация

С: 28.06.2016 0:00

До: 04.04.2017 0:00

Результат

N	Тип события	Время	Событие	Сервис
1	Информация	03.04.2017 17:44:12	Отвязка устройства	Консоль управления
Устройство успешно отвязано. Пользователь: Евгений Белов Устройство: Rutoken S:0755398982 Инициатор: INDEED-ID\ivan.ivanov				
2	Информация	03.04.2017 17:44:10	Очистка устройства	Консоль управления
Устройство успешно очищено. Пользователь: Евгений Белов Устройство: Rutoken S:0755398982 Состояние устройства: Очищено Инициатор: INDEED-ID\ivan.ivanov				
3	Информация	03.04.2017 17:43:15	Отзыв устройства	Консоль управления
Устройство успешно отозвано. Пользователь: Евгений Белов Устройство: Rutoken S:0755398982 Причина: Изъятие устройства Сертификаты: MSCA:37000000E381442BE63293C7540001000000E3 Инициатор: INDEED-ID\ivan.ivanov				
4	Информация	03.04.2017 17:42:31	Изменение политики	Консоль управления
Политика успешно изменена. Имя политики: Headquarter Инициатор: INDEED-ID\ivan.ivanov				
5	Информация	03.04.2017 15:31:23	Включение устройства	Консоль управления
Устройство успешно включено. Пользователь: Евгений Белов Устройство: Rutoken S:0755398982 Инициатор: INDEED-ID\ivan.ivanov				
6	Информация	03.04.2017 15:31:09	Изменение политики	Консоль управления
Политика успешно изменена. Имя политики: Headquarter Инициатор: INDEED-ID\ivan.ivanov				
7	Информация	03.04.2017 13:07:27	Отвязка устройства	Консоль управления
Устройство успешно отвязано. Пользователь: Евгений Белов Устройство: Rutoken ECP:0756770190 Инициатор: INDEED-ID\ivan.ivanov				
8	Информация	03.04.2017 13:07:26	Очистка устройства	Консоль управления
Устройство успешно очищено. Пользователь: Евгений Белов Устройство: Rutoken ECP:0756770190 Состояние устройства: Очищено Инициатор: INDEED-ID\ivan.ivanov				

Рисунок 96 – Отчет по событиям системы Indeed CM в формате PDF.

Список событий Indeed CM

Таблица 8 – События Indeed CM.

Тип	Событие	Текст
Информация	Добавление устройства	Устройство успешно добавлено. Устройство: Инициатор:
Ошибка	Добавление устройства	Произошла ошибка при добавлении устройства. Устройство: Инициатор: Сообщение об ошибке:
Информация	Удаление устройства	Устройство успешно удалено. Устройство: Инициатор:
Ошибка	Удаление устройства	Произошла ошибка при удалении устройства. Устройство: Инициатор: Сообщение об ошибке:
Информация	Назначение устройства	Устройство успешно назначено. Пользователь: Политика: Устройство: Инициатор:
Ошибка	Назначение устройства	Произошла ошибка при назначении устройства. Пользователь: Устройство: Инициатор: Сообщение об ошибке:
Информация	Отвязка устройства	Устройство успешно отвязано. Пользователь: Устройство: Инициатор:
Ошибка	Отвязка устройства	Произошла ошибка при отвязке устройства. Пользователь: Устройство: Инициатор: Сообщение об ошибке:
Информация	Выпуск устройства	Устройство успешно выпущено. Пользователь: Политика: Устройство: Сертификаты: Общие сертификаты: Отслеживаемые сертификаты: Инициатор:

продолжение таблицы на следующей странице

Тип	Событие	Текст
Ошибка	Выпуск устройства	Произошла ошибка при выпуске устройства. Пользователь: Устройство: Инициатор: Сообщение об ошибке:
Информация	Включение устройства	Устройство успешно включено. Пользователь: Устройство: Инициатор:
Ошибка	Включение устройства	Произошла ошибка при включении устройства. Пользователь: Устройство: Инициатор: Сообщение об ошибке:
Информация	Выключение устройства	Устройство успешно выключено. Пользователь: Устройство: Инициатор:
Ошибка	Выключение устройства	Произошла ошибка при выключении устройства. Пользователь: Устройство: Инициатор: Сообщение об ошибке:
Информация	Отзыв устройства	Устройство успешно отозвано. Пользователь: Устройство: Причина: Сертификаты: Инициатор:
Ошибка	Отзыв устройства	Произошла ошибка при отзыве устройства. Пользователь: Устройство: Причина: Инициатор: Сообщение об ошибке:
Информация	Обновление устройства	Устройство успешно обновлено. Пользователь: Устройство: Новые сертификаты: Обновленные сертификаты: Удаленные сертификаты: Новые общие сертификаты: Удаленные общие сертификаты: Новая политика: Инициатор:

продолжение таблицы на следующей странице

Тип	Событие	Текст
Ошибка	Обновление устройства	Произошла ошибка при обновлении устройства. Пользователь: Устройство: Инициатор: Сообщение об ошибке:
Информация	Замена устройства	Устройство успешно заменено. Пользователь: Устройство: Новое Устройство: Сертификаты: Общие сертификаты: Дата истечения: Инициатор:
Ошибка	Замена устройства	Произошла ошибка при замене устройства. Пользователь: Устройство: Новое устройство: Инициатор: Сообщение об ошибке:
Информация	Очистка устройства	Устройство успешно очищено. Пользователь: Устройство: Состояние устройства: Инициатор:
Ошибка	Очистка устройства	Произошла ошибка при очистке устройства. Пользователь: Устройство: Инициатор: Сообщение об ошибке:
Информация	Сброс PIN-кода	PIN-код устройства успешно сброшен. Пользователь: Устройство: Инициатор:
Ошибка	Сброс PIN-кода	Произошла ошибка при сбросе PIN-кода устройства. Пользователь: Устройство: Инициатор: Сообщение об ошибке:
Информация	Разблокировка устройства	Код разблокировки успешно сгенерирован. Пользователь: Устройство: Инициатор:

продолжение таблицы на следующей странице

Тип	Событие	Текст
Ошибка	Разблокировка устройства	Произошла ошибка при генерации кода разблокировки. Пользователь: Устройство: Инициатор: Сообщение об ошибке:
Информация	Изменение PIN-кода	PIN-код устройства успешно изменен. Пользователь: Устройство: Инициатор:
Ошибка	Изменение PIN-кода	Произошла ошибка при изменении PIN-кода устройства. Пользователь: Устройство: Инициатор: Сообщение об ошибке:
Информация	Изменение комментария	Комментарий устройства успешно изменен. Устройство: Комментарий: Инициатор:
Ошибка	Изменение комментария	Произошла ошибка при изменении комментария устройства. Устройство: Инициатор: Сообщение об ошибке:
Информация	Просмотр PIN-кода администратора	PIN-код администратора устройства просмотрен. Устройство: Инициатор:
Информация	Импортирование устройства	Устройство успешно импортировано. Пользователь: Устройство: Состояние: Сертификаты: Инициатор:
Ошибка	Импортирование устройства	Произошла ошибка при импортировании устройства. Устройство: Сообщение об ошибке: Инициатор:
Информация	Выпуск устройства ожидает решения	Выпуск устройства ожидает решения. Пользователь: Политика: Устройство: Сертификаты: Общие сертификаты: Отслеживаемые сертификаты: Инициатор:

продолжение таблицы на следующей странице

Тип	Событие	Текст
Информация	Обновление устройства ожидает решения	Выпуск устройства ожидает решения. Пользователь: Устройство: Новые сертификаты: Обновленные сертификаты: Удаленные сертификаты: Новые общие сертификаты: Удаленные общие сертификаты: Новая политика: Инициатор:
Информация	Замена устройства ожидает решения	Замена устройства ожидает решения. Пользователь: Устройство: Новое устройство: Сертификаты: Общие сертификаты: Дата истечения: Инициатор:
Информация	Отмена обновления устройства	Обновление устройства успешно отменено. Пользователь: Устройство: Инициатор:
Ошибка	Отмена обновления устройства	Произошла ошибка при отмене обновления устройства. Пользователь: Устройство: Инициатор: Сообщение об ошибке:
Информация	Предварительное обновление устройства	Предварительное обновление устройства успешно выполнено. Пользователь: Устройство: Отозванные сертификаты: Инициатор:
Ошибка	Предварительное обновление устройства	Произошла ошибка при предварительном обновлении устройства. Пользователь: Устройство: Инициатор: Сообщение об ошибке:
Информация	Изменение ответов на секретные вопросы	Ответы на секретные вопросы успешно изменены. Пользователь: Инициатор:
Ошибка	Изменение ответов на секретные вопросы	Произошла ошибка при изменении ответов на секретные вопросы. Пользователь: Инициатор: Сообщение об ошибке:

продолжение таблицы на следующей странице

Тип	Событие	Текст
Информация	Аутентификация	Пользователь успешно аутентифицирован. Пользователь: Инициатор:
Ошибка	Аутентификация	Произошла ошибка при аутентификации пользователя. Пользователь: Инициатор: Сообщение об ошибке:
Предупреждение	Блокировка пользователя	Пользователь заблокирован. Пользователь: Инициатор:
Информация	Разблокировка пользователя	Пользователь успешно разблокирован. Пользователь: Инициатор:
Ошибка	Разблокировка пользователя	Произошла ошибка при разблокировке пользователя. Пользователь: Инициатор: Сообщение об ошибке:
Информация	Сброс ответов на секретные вопросы	Ответы на секретные вопросы успешно сброшены. Пользователь: Инициатор:
Ошибка	Сброс ответов на секретные вопросы	Произошла ошибка при сбросе ответов на секретные вопросы. Пользователь: Инициатор: Сообщение об ошибке:
Информация	Создание политики	Политика успешно создана. Имя политики: Контейнер: Группа: Приоритет: Скопирована с: Инициатор:
Ошибка	Создание политики	Произошла ошибка при создании политики. Имя политики: Контейнер: Группа: Приоритет: Инициатор: Сообщение об ошибке:
Информация	Удаление политики	Политика успешно удалена. Имя политики: Инициатор:
Ошибка	Удаление политики	Произошла ошибка при удалении политики. Имя политики: Инициатор: Сообщение об ошибке:

продолжение таблицы на следующей странице

Тип	Событие	Текст
Информация	Изменение политики	Политика успешно изменена. Имя политики: Инициатор:
Ошибка	Изменение политики	Произошла ошибка при изменении политики. Имя политики: Инициатор: Сообщение об ошибке:
Информация	Добавление лицензии	Лицензия успешно добавлена. Тип: Действительна с: Действительна по: Количество: Инициатор:
Ошибка	Добавление лицензии	Произошла ошибка при добавлении лицензии. Инициатор: Сообщение об ошибке:
Информация	Удаление лицензии	Лицензия успешно удалена. Тип: Действительна с: Действительна по: Количество: Инициатор:
Ошибка	Удаление лицензии	Произошла ошибка при удалении лицензии. Инициатор: Сообщение об ошибке:
Информация	Добавление типа устройства	Тип устройства успешно добавлен. Имя: Инициатор:
Ошибка	Добавление типа устройства	Произошла ошибка при добавлении типа устройства. Имя: Инициатор: Сообщение об ошибке:
Информация	Удаление типа устройства	Тип устройства успешно удален. Имя: Инициатор:
Ошибка	Удаление типа устройства	Произошла ошибка при удалении типа устройства. Имя: Инициатор: Сообщение об ошибке:
Информация	Изменение типа устройства	Тип устройства успешно изменен. Имя: Инициатор:
Ошибка	Изменение типа устройства	Произошла ошибка при изменении типа устройства. Имя: Инициатор: Сообщение об ошибке:

продолжение таблицы на следующей странице

Тип	Событие	Текст
Ошибка	Отправка уведомления	Произошла ошибка при отправке уведомления. Сообщение об ошибке:
Информация	Добавление СКЗИ	СКЗИ успешно добавлено. Пользователь: Наименование: Серийный номер: Номер экземпляра: Инициатор:
Ошибка	Добавление СКЗИ	Произошла ошибка при добавлении СКЗИ. Пользователь: Наименование: Серийный номер: Номер экземпляра: Инициатор: Сообщение об ошибке:
Информация	Обновление СКЗИ	СКЗИ успешно обновлено. Пользователь: Наименование: Серийный номер: Номер экземпляра: Инициатор:
Ошибка	Обновление СКЗИ	Произошла ошибка при обновлении СКЗИ. Пользователь: Наименование: Серийный номер: Номер экземпляра: Инициатор: Сообщение об ошибке:
Информация	Уничтожение/изъятие СКЗИ	СКЗИ успешно уничтожено/изъято. Пользователь: Наименование: Серийный номер: Номер экземпляра: Инициатор:
Ошибка	Уничтожение/изъятие СКЗИ	Произошла ошибка при уничтожении/изъятии СКЗИ. Пользователь: Наименование: Серийный номер: Номер экземпляра: Инициатор: Сообщение об ошибке:
Информация	Добавление AirKey к компьютеру	AirKey был добавлен к компьютеру. Устройство: Компьютер:
Ошибка	Добавление AirKey к компьютеру	Произошла ошибка при добавлении AirKey к компьютеру. Устройство: Компьютер: Сообщение об ошибке:

продолжение таблицы на следующей странице

Тип	Событие	Текст
Информация	Создание кода подключения AirKey к компьютеру	Код подключения AirKey к компьютеру успешно создан. Устройство: Компьютер:
Ошибка	Создание кода подключения AirKey к компьютеру	Произошла ошибка при создании кода подключения AirKey к компьютеру. Устройство: Компьютер: Сообщение об ошибке:
Информация	Удаление AirKey от компьютера	AirKey был удален от компьютера. Устройство: Компьютер:
Ошибка	Удаление AirKey от компьютера	Произошла ошибка при удалении AirKey от компьютера. Устройство: Компьютер: Сообщение об ошибке:

Indeed CM Self Service

Приложение Self Service предназначено для пользователей Indeed CM и позволяет им самостоятельно осуществить определенные операции с устройством. Доступ к приложению осуществляется по адресу https://<адрес сервера Indeed CM>/icmservice.

Набор действий с устройством, доступных пользователю в приложении Self Service определяется администратором Indeed CM в приложении Management Console в разделе Конфигурация > Политики > Поведение.

Ниже приведены все возможные действия, доступные для пользователя:

- Выпуск устройства (в т.ч. виртуальной карты AirKey)
- Включение и выключение устройства
- Отзыв устройства
- Смена PIN-кода устройства
- Обновление содержимого устройства
- Установка секретных вопросов
- Изменение ответов на секретные вопросы
- Просмотр информации о пользователе каталога КриптоПро
- Просмотр содержимого устройства и печать сертификата или запроса на сертификат

После входа пользователя в сервис самообслуживания ему доступна информация о себе, сгруппированная в виде таблицы с полями: имя, логин, электронная почта, телефон и фото (Рисунок 97).

Информация о пользователе (имя, имя для входа в домен, электронная почта, телефон и фото) добавляется в систему Indeed CM автоматически из профиля пользователя в Active Directory. Изменения, внесенные в профиль пользователя в Active Directory, моментально отображаются и в Indeed CM Self Service.

Евгений Белов

Логин INDEED-ID\Евгений Белов
E-mail belov@indeed.ru
Телефон +7 (905) 2885823

Изменить ответы на секретные вопросы Пользователь КриптоПро 2.0

Ваши устройства

Выберите устройство для выполнения необходимой операции

Rutoken ECP SC, 0862287369 Евгений Белов Выпущено

Действия Содержимое

Политика была обновлена. Обновите устройство.

Обновить содержимое устройства
Обновить содержимое устройства, если срок его действия истекает, истек или была обновлена политика

Временно выключить устройство
Временно выключить устройство, если оно не нужно в течение продолжительного периода времени

Сообщить о том, что устройство неисправно или утеряно
Отозвать устройство для предотвращения использования ваших учетных данных

Сбросить PIN-код устройства
Сбросить PIN-код устройства, если оно заблокировано или вы предполагаете, что кто-либо другой узнал его

AirKey, c6e7cd5a7ab845ee Евгений Белов Выпущено

Выпустить устройство

Рисунок 97 – Карточка пользователя с полным набором действий.

При первом входе в приложение Self Service пользователю может быть предложено выполнить следующие действия:

- Установить секретные вопросы (если для него уже выпущено устройство) – Рисунок 98.
- Выпустить устройство самостоятельно (если выпущенных устройств нет, и выпуск разрешен настройками политики использования устройств) – Рисунок 99.

Евгений Белов

Логин	INDEED-ID\Евгений Белов
E-mail	belov@indeed.ru
Телефон	+7 (905) 2885823

Для работы с системой задайте ответы на секретные вопросы

Секретные вопросы необходимы для подтверждения операций с вашими устройствами

Секретный вопрос

Выберите вопрос

Ответ

OK

Рисунок 98 – Установка секретных вопросов при первом входе в приложение Self Service.

Если политикой использования устройств пользователю разрешено выбирать сертификаты при выпуске, то список таких сертификатов будет отображен в диалоге выпуска устройства (Рисунок 99).

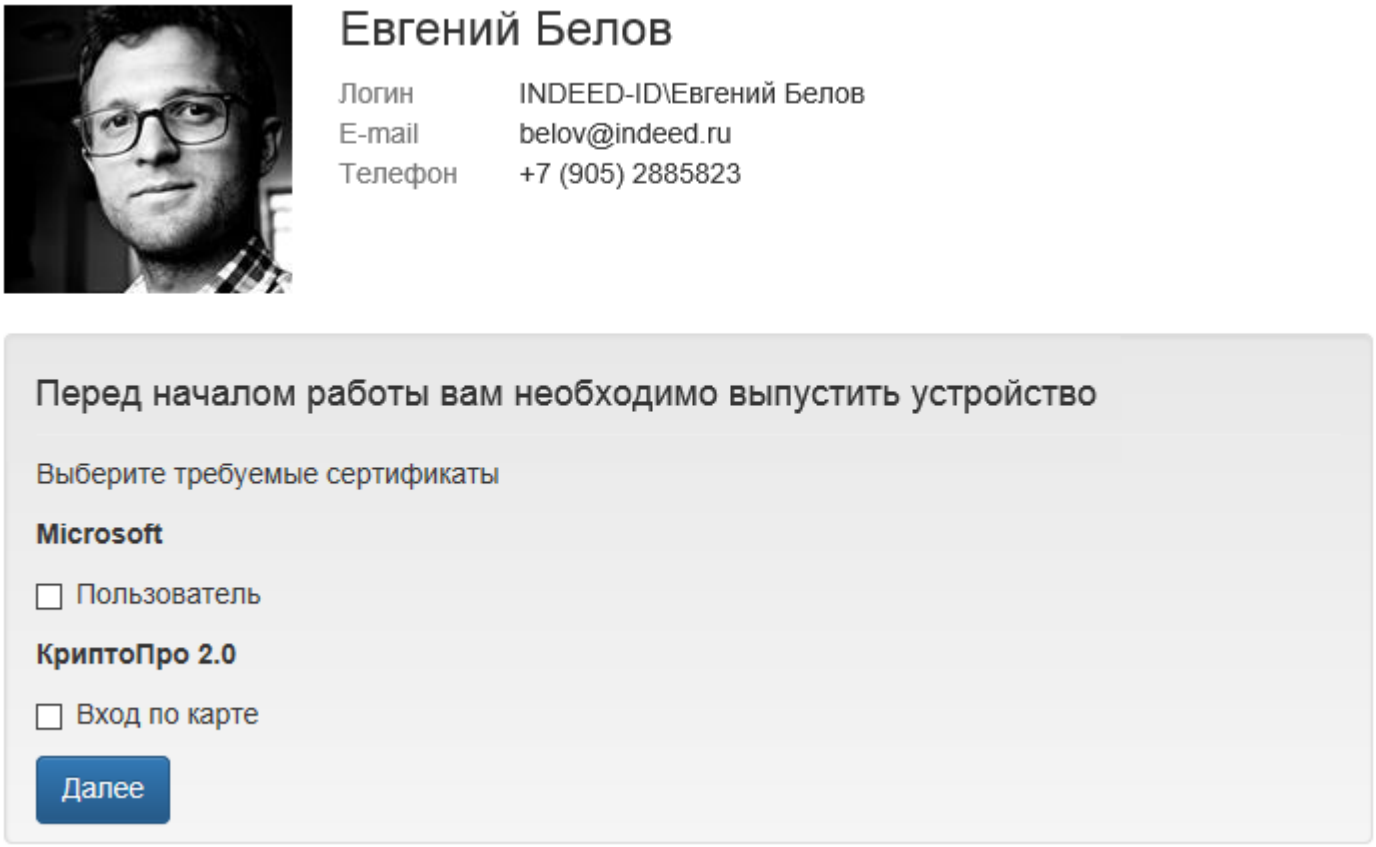

Рисунок 99 – Выпуск устройства при первом входе в приложение Self Service. Пользователю разрешены самостоятельный выпуск устройств и выбор сертификатов.

При выпуске устройство может быть инициализировано, если соответствующая опция включена в политике использования устройств (Рисунок 100).

Евгений Белов

Логин INDEED-ID\Евгений Белов
E-mail belov@indeed.ru
Телефон +7 (905) 2885823

Перед началом работы вам необходимо выпустить устройство

Задайте имя устройства

Устройство будет проинициализировано. Все данные на устройстве будут потеряны

Имя устройства

Евгений Белов

Номер документа

Номер документа

Устройство

ARDS JaCarta 0: IDProtect (X)

Дополнительно

PIN-код администратора

PIN-код администратора

PIN-код администратора (ГОСТ)

PIN-код администратора (ГОСТ)

Выпустить

Рисунок 100 – Выпуск устройства при первом входе в приложение Self Service. Пользователю разрешен самостоятельный выпуск устройств, включена обязательная инициализация устройства перед выпуском и ведется учет СКЗИ.

В случае ведения учета СКЗИ в Indeed CM при выпуске устройства необходимо указать номер документа, на основании которого осуществляется выпуск средства криптографической защиты.

Введите PIN-коды администратора (если устройство не добавлено в Indeed CM) и пользователя (доступно при отключенной инициализации устройства) в разделе **Дополнительно**. Значения PIN-кода пользователя и администратора могут быть пустыми. В этом случае они будут установлены в соответствии со значением в разделе **Конфигурация – Типы устройств**. Поддерживается ввод PIN-кодов для нескольких областей (например, для PKI и ГОСТ на устройствах JaCarta). Для выпуска устройства нажмите **Выпустить** (Рисунок 100).

Если политикой использования устройств разрешена генерация случайного PIN-кода пользователя и его отображение в сервисе самообслуживания, то по завершению процесса выпуска устройства пользователь увидит свой PIN-код (Рисунок 101).

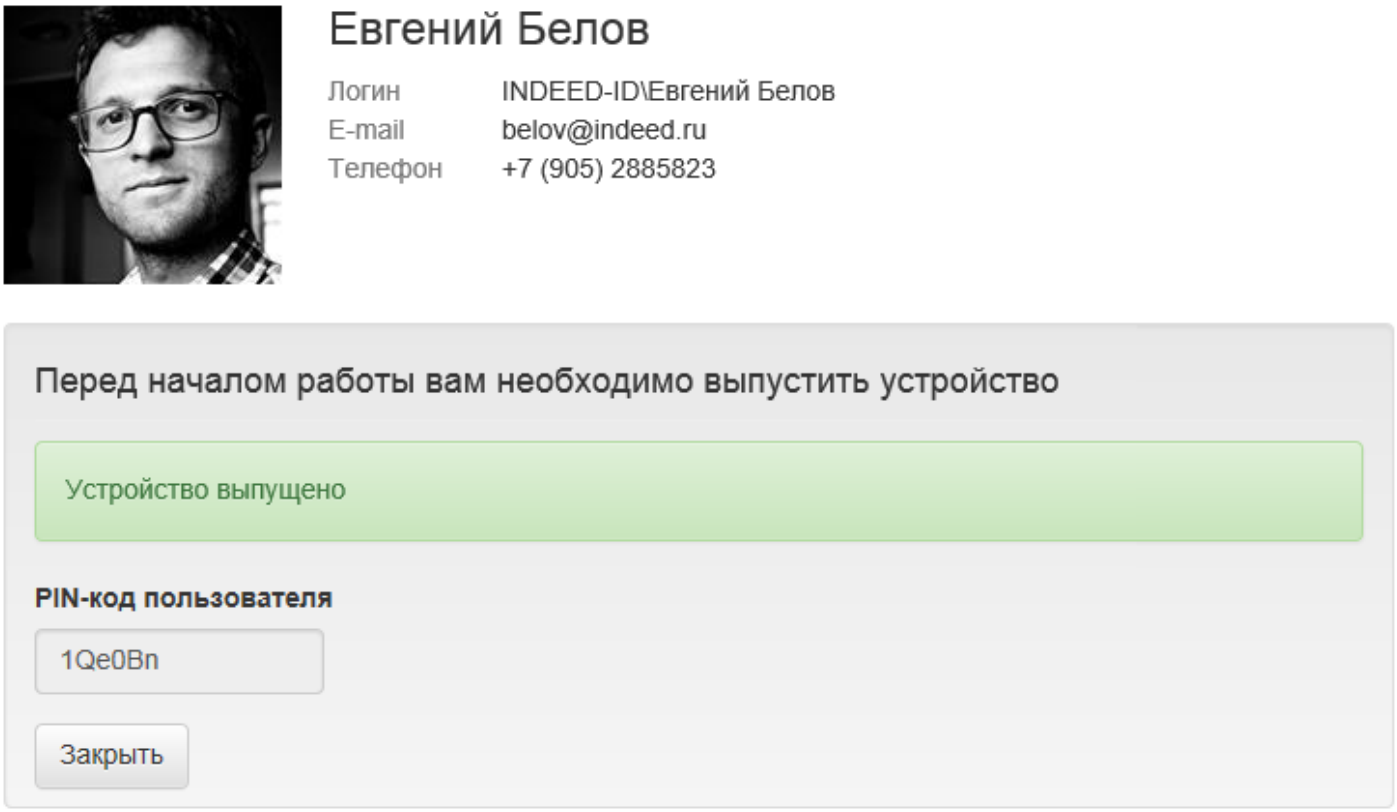

Рисунок 101 – Выпуск устройства при в приложении Self Service. Пользователю разрешен самостоятельный выпуск устройства, включена генерация случайного PIN-кода пользователя и его отображение.

PIN-код может быть отправлен на электронную почту пользователя или его руководителя, если в политике использования устройств настроены соответствующие почтовые уведомления.

Если настройками системы разрешено отображение содержимого устройства в Self Service[33], то в свойствах выпущенного устройства будет доступна вкладка **Содержимое**, содержащая сведения о сертификатах, находящихся на устройстве (Рисунок 102).

[33]Опция **Отображать содержимое устройства в сервисе самообслуживания** в разделе **Функции системы** Мастера настройки Indeed Card Management.

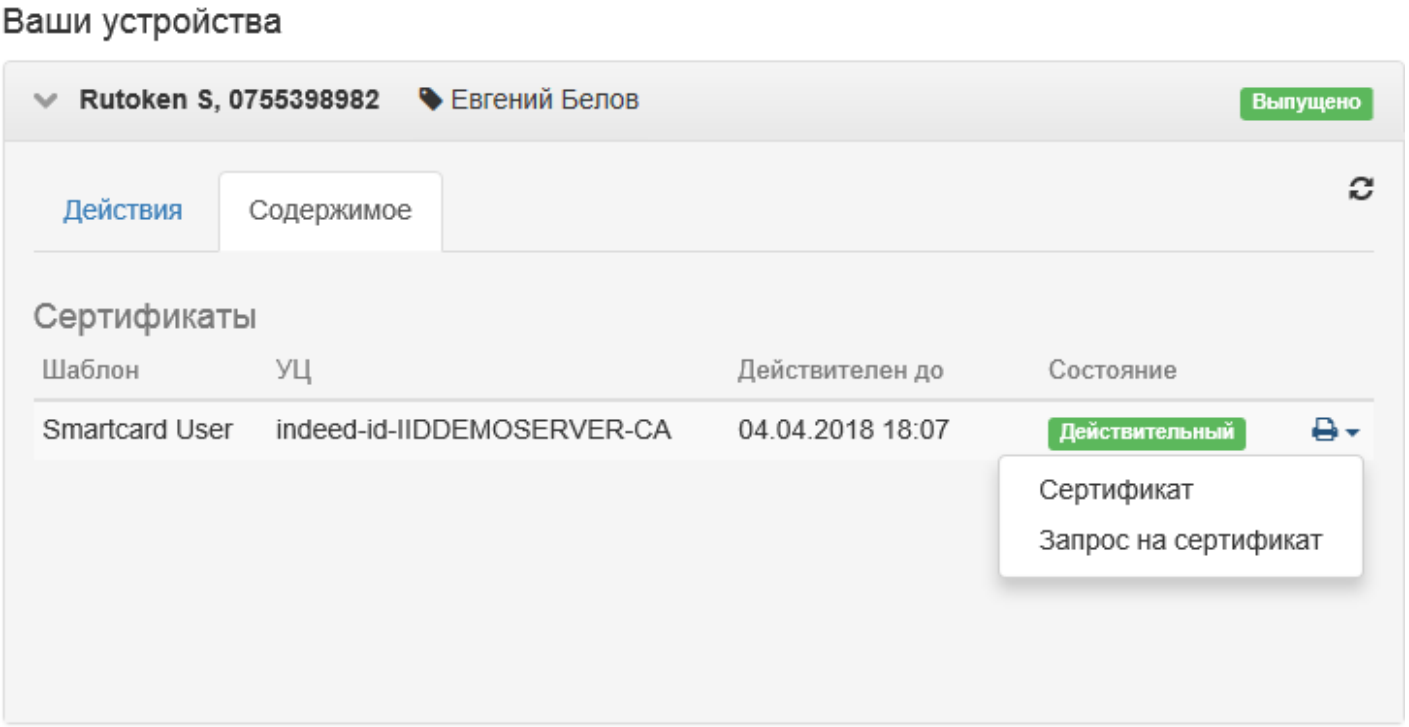

Рисунок 102 – Содержимое устройства пользователя.

При необходимости пользователь может распечатать сведения о сертификате и(или) его запросе. Печать осуществляется по нажатию кнопки (Рисунок 102).

Indeed CM Remote Self Service

Приложение предназначено для выполнения операций с устройством, без его подключения к компьютеру пользователя. Доступно по адресу https://<адрес сервера Indeed CM >/icmremote и может быть опубликовано для доступа из Интернет. Для использования Remote Self Service пользователю необходимо ввести своё имя и символы с изображения (Рисунок 103).

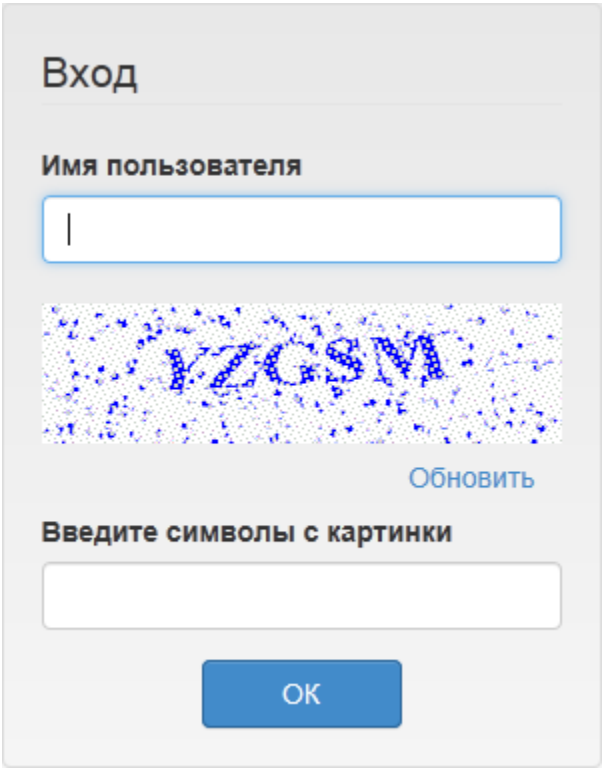

Рисунок 103 – Окно входа в Remote Self Service.

Для доступа к карточке пользователя требуется аутентификация по секретным вопросам (Рисунок 104).

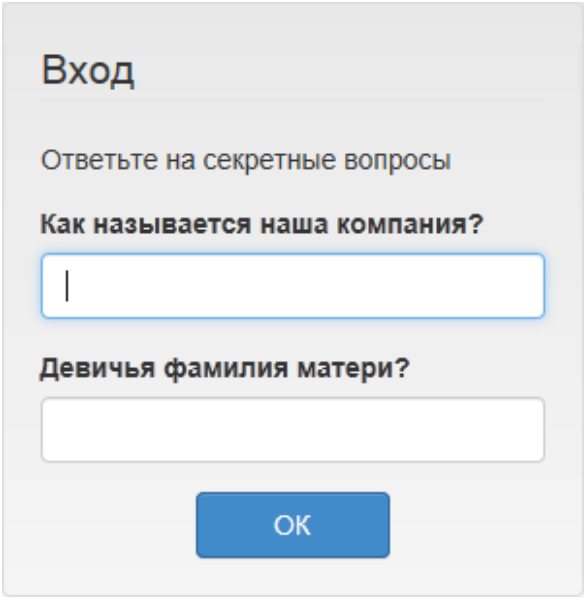

Рисунок 104 – Аутентификация пользователя в Remote Self Service.

В случае указания верных ответов на секретные вопросы пользователь получает доступ к управлению своими устройствами (Рисунок 105).

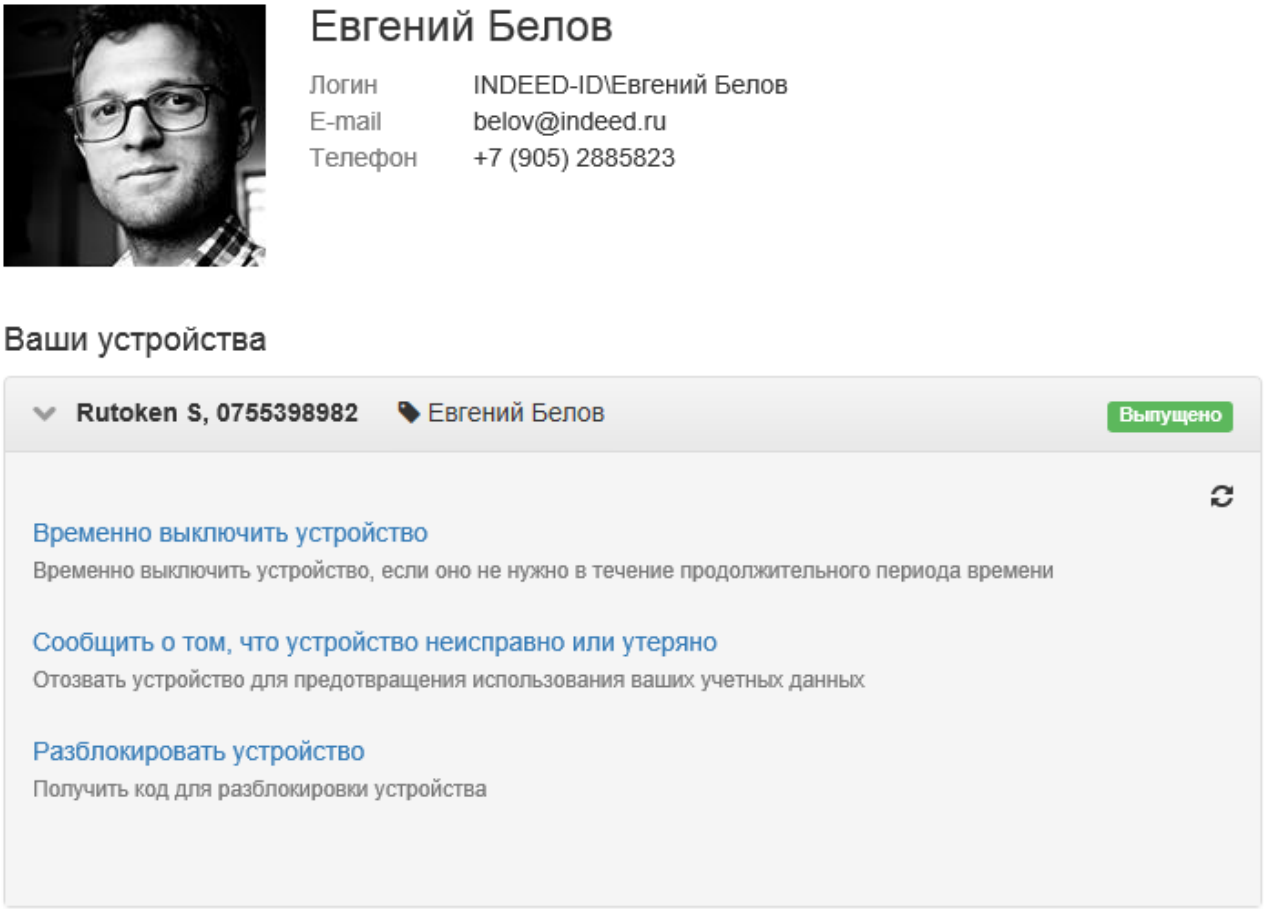

Рисунок 105 – Карточка пользователя в Remote Self Service.

Сбор программных логов

Сбор логов клиентской части

Наличие программных логов позволяет специалистам службы поддержки определить причины возможных проблемных ситуаций и принять меры к их устранению. Сбор программных логов осуществляется с помощью утилиты GetLog, поставляемой в составе дистрибутива Indeed Card Management. Для получения подробной информации обратитесь к документу *Indeed-Id GetLog. Руководство пользователя.pdf*.

Сбор логов web-сервисов на сервере

1. Перейдите в каталог сервиса, логи которого необходимо получить (icm, icmservice, icmremote, credprovapi, icmapi). Путь по умолчанию %SystemDrive%\inetpub\wwwroot\. Каталог сервиса CardMonitor располагается в %ProgramFiles%\Indeed CM\CardMonitor.
2. Откройте файл **Web.nlog** (**NLog.config** для Card Monitor) в текстовом редакторе, например, в Блокнот, запущенном от имени администратора, и измените параметр minlevel="Off" на "Info":

   ```
   <logger name="*" minlevel="Info" writeTo="file" />
   ```

3. Сохраните изменения в файле.
4. Воспроизведите сценарий, логи которого необходимо получить.
5. Перейдите в каталог Logs, расположенный в каталоге web-сервиса и убедитесь в том, что в нем появились подкаталоги с файлами отладочной информации.
6. Пришлите каталог Logs со всем его содержимым на адрес службы технической поддержки **support@indeed-id.com** с описанием воспроизведения проблемы.
7. Для отключения логирования измените значение параметра minlevel с Info на Off и сохраните изменения в файле.

Часто задаваемые вопросы

Ознакомиться со списком часто задаваемых вопросов и ответов на них можно в **Базе знаний** по продукту Indeed Card Management.