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-Id ESSO Агент

Руководство по установке и эксплуатации

версия 6.3.0

Содержание

Введение

Приветствуем и благодарим за приобретение программного комплекса Indeed ID. Это Руководство поможет вам правильно подготовить и выполнить установку **Indeed-Id ESSO Агент**.

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.

О продукте Indeed-Id ESSO Агент

Indeed Enterprise Single Sign-On реализует технологию единого доступа Single Sign On в информационные системы организации: централизованно хранит пароли приложений пользователя и выполняет автоматическую подстановку пароля в скрытом виде при необходимости доступа в приложение или выполнения других действий, требующих аутентификации. Indeed-Id ESSO Агент упрощает процедуру аутентификации в приложениях исключая необходимость ручного ввода пароля и периодической смены пароля пользователем.

Поддерживаемые приложения

Технология доступа Indeed Enterprise Single Sign-On применяется для windows и web приложений и настраивается без программного вмешательства в серверную или клиентскую часть целевого приложения. Поддержка нового приложения подразумевает создание специального шаблона в формате .xml. В шаблоне указывается, какие формы приложения будут контролироваться. Контроль доступа выражается в повторном запросе аутентификации, заполнении полей регистрационными данными (имя пользователя и пароль), активации нужных элементов управления (нажатие кнопки «Вход»), запись события в журнал и т.п.

Поддерживаемые технологии аутентификации

В дополнение к стандартной технологии аутентификации, реализованной в большинстве продуктов Single Sign-On, - универсальному паролю мастер-паролю, Indeed-Id Enterprise SSO поддерживает альтернативные технологии аутентификации.

К ним относятся двухфакторная, биометрическая, сертификаты, бесконтактные карты, одноразовые пароли, sms-технологии и др. Для каждой категории пользователей Indeed-Id Enterprise SSO подбирается собственная технология аутентификации. Поддерживается комбинация нескольких технологий:

- технология аутентификации, адаптированная для работы в удаленном режиме
- мультифакторная аутентификация.

Установка и настройка

Системные требования

Аппаратные требования к рабочим станциям пользователей

- Не менее 50 МБ свободного дискового пространства
- Аппаратные требования совпадают с требованиями, предъявляемыми к операционным системам, на которых функционирует ПО
- Веб-браузеры:
  - Internet Explorer 8 и выше
  - Mozilla Firefox 52.6 и выше
  - Google Chrome 49.0 и выше
- USB-порт для подключения устройства аутентификации.

Поддерживаемые операционные системы

- Windows Server 2008 SP2 32/64bit (с обновлением KB980368)
- Windows Server 2008 R2 SP1
- Windows Server 2012/2012 R2
- Windows Server 2016
- Windows XP SP2 64 bit, SP3 32bit
- Windows 7 SP1 32/64bit
- Windows 8.1 32/64bit
- Windows 10 32/64bit

Настройки межсетевого экрана

Задайте следующие настройки межсетевого экрана на сервере Indeed ESSO и на рабочих станциях с установленным Indeed-Id ESSO Агент:

1. **Откройте порт 53 DNS (TCP и UDP)** для всех процессов в обоих направлениях. Этот порт используется для определения наличия сети.
2. **Откройте порт 3268 Microsoft Global Catalog (TCP)** для всех процессов в обоих направлениях. Этот порт используется для поиска серверов Indeed ESSO.

3. Если при установке сервера Indeed ESSO выбрана опция **Использовать статический порт**, откройте указанный порт TCP (по умолчанию, 23809) для всех процессов в обоих направлениях. Этот порт используется для обмена данными между рабочими станциями пользователей и серверами Indeed ESSO.

4. **Запретите IPS (Intrusion Prevention System)**. При разрешенном IPS межсетевым экраном блокируется исходящий запрос на неизвестный DCOM интерфейс. В этом случае соединение с сервером Indeed-Id не будет установлено.

5. **Открыть порт 135 (RPC)** для всех процессов в обоих направлениях. Этот порт используется для обмена данными между рабочими станциями пользователей и Indeed-Id Enterprise Server.

6. **Открыть порт 389 (LDAP)** для всех процессов в обоих направлениях. Этот порт используется для получения доступа в Active Directory (в т.ч. при поиске Indeed-Id Enterprise Server).

Установка Indeed-Id ESSO Агент

Установка компонента выполняется на рабочих местах пользователей. Для установки компонента требуются права Локального администратора.

Для развертывания Indeed-Id Enterprise SSO Агент на рабочих станциях пользователей в автоматическом режиме удобно использовать механизм групповых политик (Microsoft Group Policy). Или любой другой инструмент, позволяющий массово распространять и устанавливать msi-пакеты на рабочие станции пользователей (например, Microsoft System Center Configuration Manager). Подробнее со способами распространения компонентов системы Indeed-Id в автоматическом режиме можно ознакомиться в документе Indeed-Id. Руководство по развертыванию системы.pdf.

1. Запустите программу установки **IndeedID.Enterprise SSO.Agent.msi** и следуйте указаниям Мастера установки.
2. После завершения установки компонента потребуется перезагрузка системы. Нажмите **Да**, чтобы выполнить перезагрузку сразу, или **Нет**, чтобы сделать это позднее вручную.

Настройка web-плагина Indeed ESSO

При работе с web-приложениями Indeed-Id ESSO Агент использует web-плагин для браузеров Internet Explorer, Mozilla Firefox и Google Chrome.

Internet Explorer

Надстройка Indeed-Id Enterprise SSO Helper для Internet Explorer устанавливается вместе с Indeed-Id ESSO Агент. Для работы расширения включите его в браузере (Рисунок 1). Если после установки Indeed-Id ESSO Агент надстройка не появилась в браузере выполните следующие действия:

1. Перейдите в **Свойства браузера** (Internet options)-> **Дополнительно** (Advanced) -> раздел **Обзор** (Browsing) и включите опцию **Разрешение сторонних расширений обозревателя** (Enable third-party browser extensions).

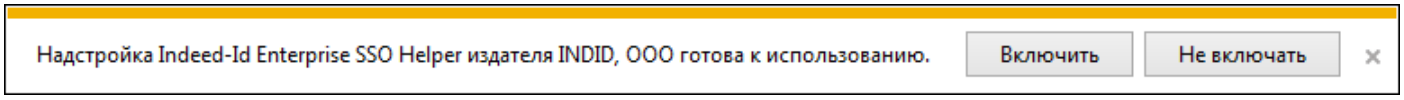

Рисунок 1 – Надстройка для браузера Internet Explorer.

2. На серверных операционных системах в дополнение к п.1 перейдите в **Диспетчер серверов** (Server manager) -> **Локальный сервер**[1] (Local server) и отключите **Конфигурацию усиленной безопасности Internet Explorer** (IE ESC).

Для массовой настройки параметров работы с надстройками в Internet Explorer используйте групповые политики Windows.
Политики располагаются в **Редакторе локальной групповой политики** (Local Group Policy Editor, gpedit.msc) в разделе **Конфигурация пользователя** (User Configuration)**Административные шаблоны** (Administrative Templates)**Компоненты Windows** (Windows Components)**Internet Explorer**.

1. Включите политику **Автоматически активировать новые установленные надстройки** (Automatically activate newly installed add-ons) для автоматического включения web-плагина.
2. Для запрета выключения надстроек пользователями включите политику **Не разрешать пользователям включать и отключать надстройки** (Do not allow users to enable or disable add-ons).

Mozilla Firefox
Расширение Indeed Id ESSO устанавливается вместе с Indeed-Id ESSO Агент. Для работы расширения включите его в браузере (Рисунок 2).

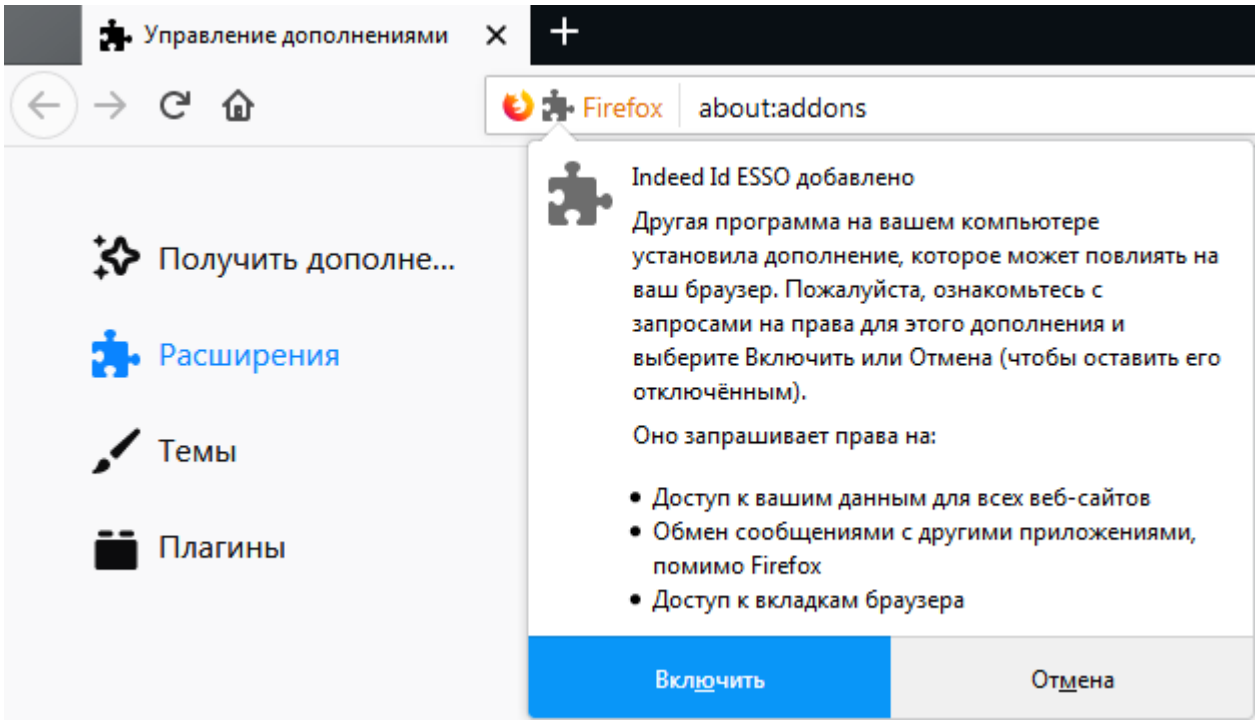

Рисунок 2 – Дополнение для браузера Mozilla Firefox.

[1]Раздел **Сведения системы безопасности** (Security Information) для Windows Server 2008R2.

Google Chrome

Расширение Indeed Id ESSO устанавливается в ручном или автоматическом режиме, через механизм групповых политик Microsoft Windows.

Установка из Интернет-магазина Chrome:

1. Установите Indeed-Id ESSO Агент на рабочую станцию, обладающей доступом в Интернет.
2. Запустите Google Chrome. Загрузка расширения произойдет автоматически в течение 1 минуты. После загрузки расширения доступ к интернету не требуется. Для работы расширения включите его в браузере (Рисунок 2).

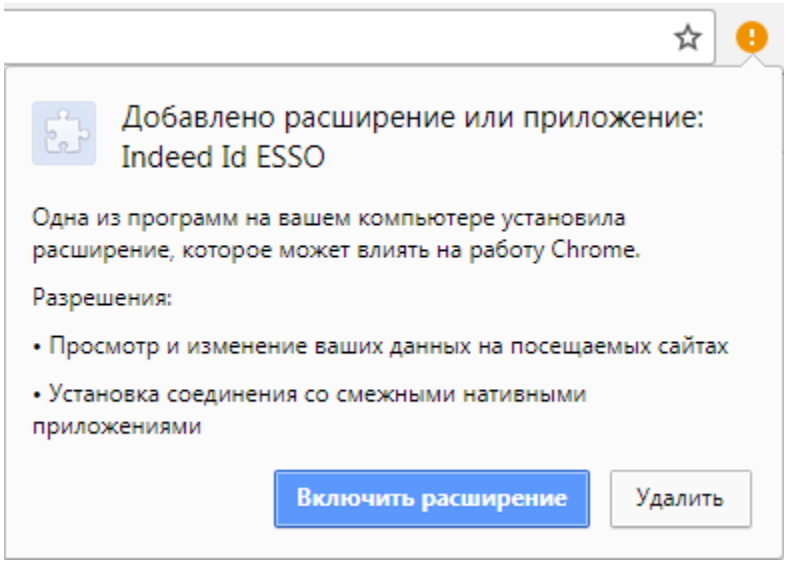

Рисунок 3 – Расширение для браузера Google Chrome.

Загрузку и включение расширения потребуется производить для каждой сессии пользователя в Windows. Если расширение было удалено из браузера вручную, то для повторной установки загрузите его из **Интернет-магазина Chrome**[2].

Установка через механизм групповых политик:[3]

Расширение Indeed Id ESSO, распространяемое групповыми политиками, устанавливается для всех пользователей рабочей станции. Для установки не требуется доступ в Интернет.

Для настройки групповой политики на установку расширения Indeed Id ESSO выполните следующие действия:

1. Создайте в **Диспетчере служб IIS** (IIS Manager) web-приложение с произвольным именем, например **chromeplugin**, определите для него пул приложений **DefaultAppPool** и **Анонимную проверку подлинности** (Anonymous Authentication).
2. В каталог приложения поместите файлы **lcjenjmcehnkfkghcflkfialplejjkdj.crx** и **update.xml** (располагаются в дистрибутиве Indeed Enterprise Single Sign-On\<версия>\Misc\ChromePlugin).
3. В разделе **Типы MIME** (MIME Types) веб-сайта, в котором находится приложение **chromeplugin**, добавьте новый тип с расширением **.crx** и описанием **application/chrome** (Рисунок 4).

[2]Доступно по ссылке https://chrome.google.com/webstore/detail/indeed-id-esso/lcjenjmcehnkfkghcflkfialplejjkdj

[3]Не поддерживается для Windows XP.

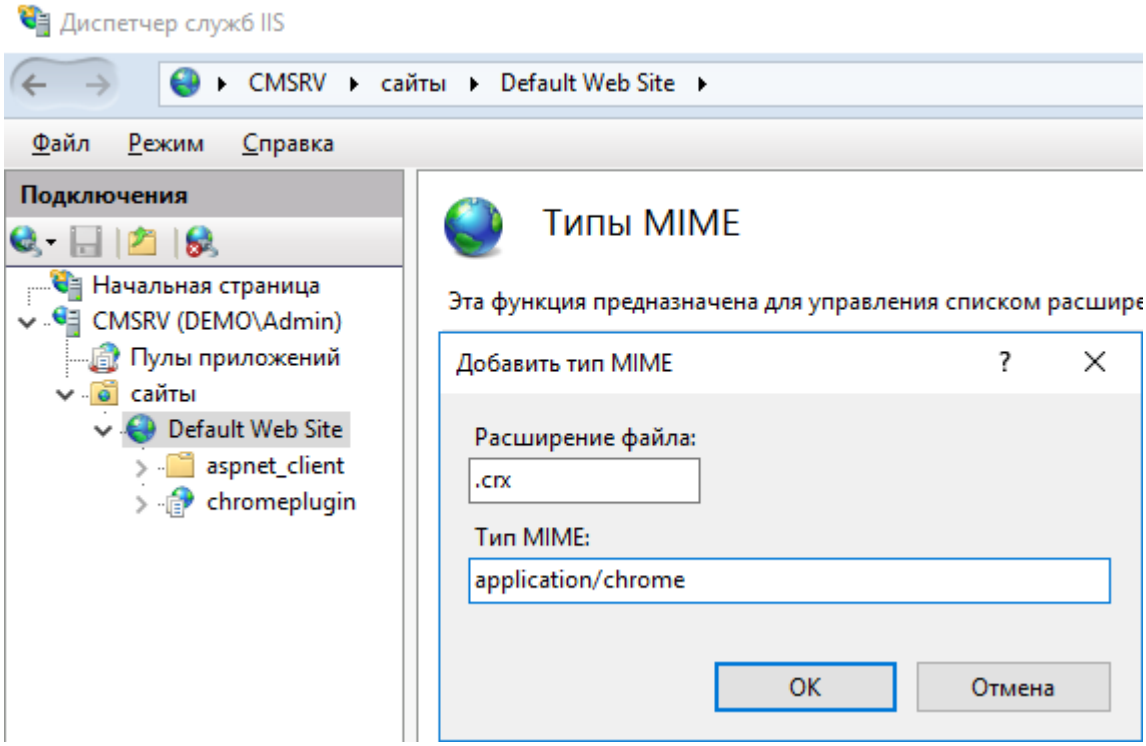

Рисунок 4 – Тип MIME для установки расширения в Google Chrome.

4. Настройте безопасное https соединение для приложения **chromeplugin** и убедитесь что к нему можно обратиться с рабочих станций пользователей.
5. Добавьте шаблоны[4] adm/admx в локальное/центральное хранилище административных шаблонов контроллера домена и создайте новый объект групповой политики в оснастке **Управление групповой политикой** (Group Policy Management) с произвольным именем.
6. Откройте для редактирования созданный объект групповой политики и перейдите в раздел **Конфигурация компьютера** (Computer Configuration) -> **Административные шаблоны** (Administrative Templates) -> **Google** -> **Google Chrome** -> **Расширения** (Extensions).
7. Включите политику **Создать список приложений и расширений, устанавливаемых принудительно** (Configure the list of force-installed apps and extensions) и укажите идентификатор расширения (указан в имени файла .crx) и путь к .xml файлу в каталоге созданного в п.2 web-приложения chromeplugin (Рисунок 5). Сохраните внесенные изменения.

[4]Доступны по ссылке http://dl.google.com/dl/edgedl/chrome/policy/policy_templates.zip

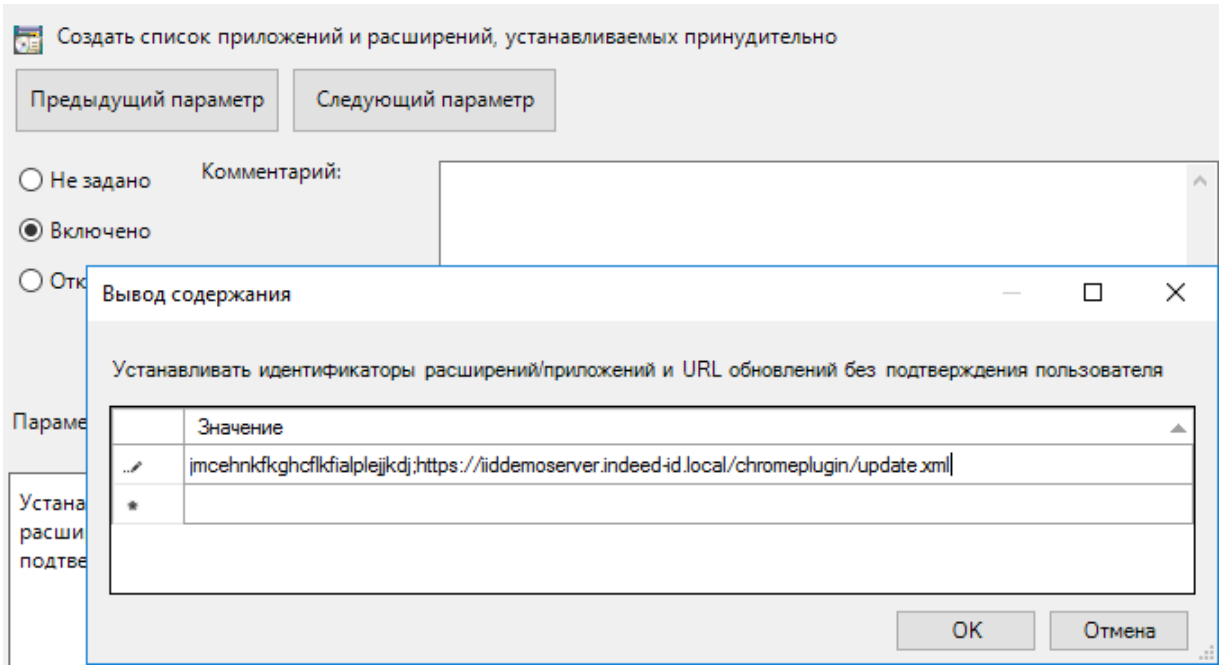

Рисунок 5 – Настройка списка принудительно устанавливаемых расширений Google Chrome.

8. Включие политику **Настроить источники для установки расширений, приложений и пользовательских скриптов** (Configure extension, app, and user script install sources) и укажите адрес сервера, на котором развернуто созданное в п.2 web-приложение chromeplugin (Рисунок 6). Сохраните изменения.

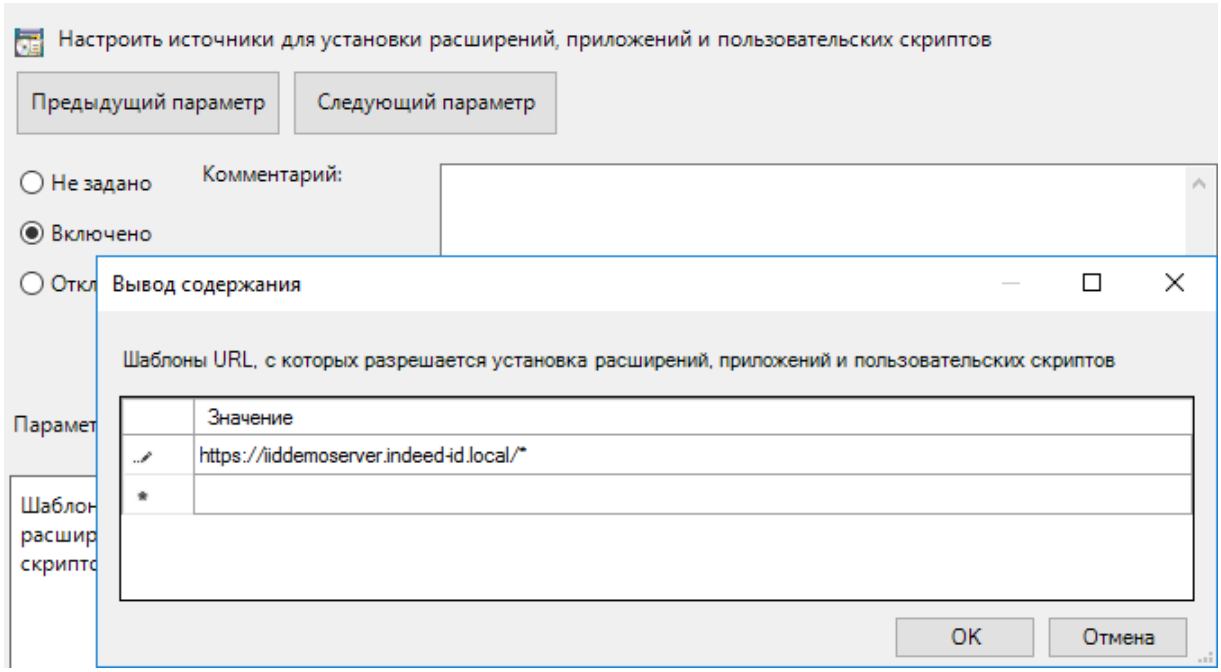

Рисунок 6 – Настройка источника для установки расширений Google Chrome.

9. Распространите действие объекта групповой политики на рабочие станции пользователей с установленным Indeed-Id ESSO Агент.

10. Расширение автоматически загрузится и установится после применения групповой политики к рабочей станции Может потребоваться до нескольких минут для того, чтобы оно отобразилось в списке установленных в браузере. Установленное через групповые политики расширение отмечено соответствующим символом (Рисунок 7).

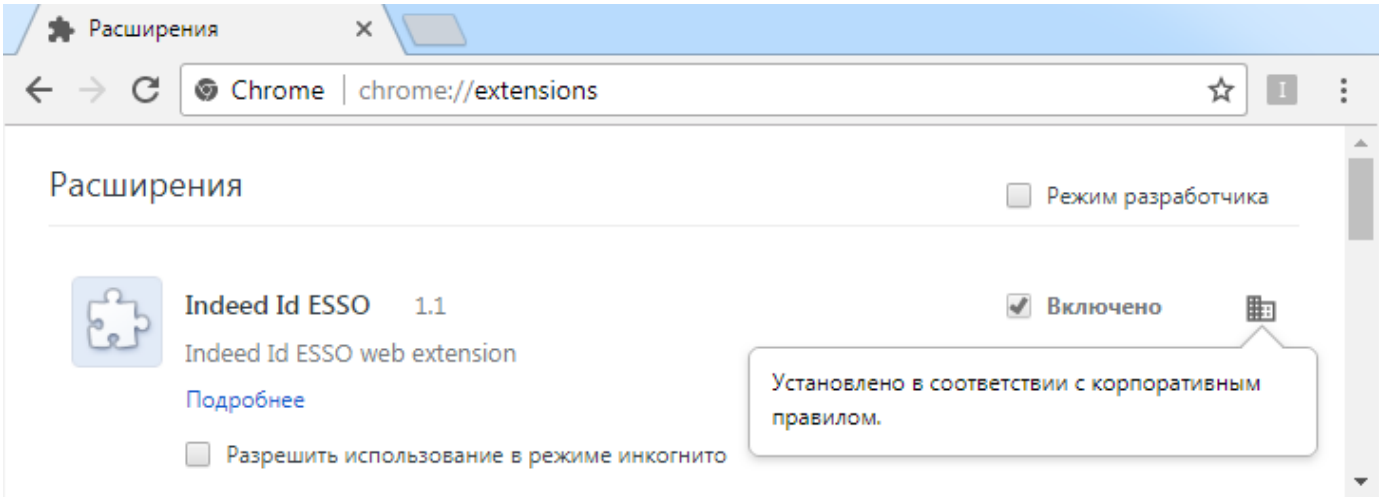

Рисунок 7 – Установленное при помощи групповых политик расширение Indeed Id ESSO.

Работа Indeed Enterprise Single Sign-On

Работа Indeed Enterprise Single Sign-On заключается в отслеживании запуска приложений и автоматическом заполнении полей и форм данными, необходимыми для получения доступа в приложение: имя пользователя, пароль и т.п. Автоматическое заполнение полей данными происходит только после подтверждения личности пользователя с применением поддерживаемой технологии аутентификации. Таким образом, Indeed Enterprise Single Sign-On избавляет пользователей от необходимости запоминания, записи, хранения, ручного ввода паролей для выполнения входа в приложение. Благодаря централизованному хранению SSO-профилей пользователи получают доступ в приложения с любой рабочей станции, где установлен компонент Indeed-Id ESSO Агент. Поддержка в Indeed-Id ESSO Агент технологий аутентификации, специально адаптированных для использования в терминальной среде и не требующих установки дополнительного оборудования, дает возможность работать на «неподготовленном» компьютере и использовать тонкие клиенты на базе Windows CE, Linux, Wyse и т.п.

Единый доступ в приложения по технологии аутентификации Indeed

Доступ в приложения с использованием аутентификатора становится возможен после настройки учетной записи приложения, профиля пользователя и регистрации аутентификатора. Для получения доступа в приложение с использованием технологии аутентификации Indeed-Id выполните следующие действия:

1. Выполните вход на рабочую станцию. В панели задач отобразится всплывающее сообщение об открытии SSO-сессии (Рисунок 8).

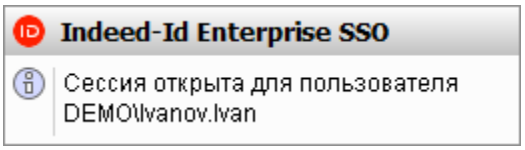

Рисунок 8 – Старт сессии пользователя Indeed Enterprise Single Sign-On.

2. Indeed-Id ESSO Агент запускается автоматически при входе в операционную систему. Для запуска вручную выберите пункт **Indeed-Id** > **Enterprise SSO** > **Enterprise SSO - Агент** в меню **Программы**.

Выбор целевого приложения

Для выбора целевого приложения выполните одно из следующих действий:

1. Нажмите [**Ctrl**]+[**Alt**]+[**Q**] или откройте приложение Indeed-Id Enterprise SSO Агент двойным щелчком по иконке в области уведомлений Windows.
2. Нажатием правой кнопки мыши на иконку в области уведомлений Windows вызовите контекстное меню приложения Indeed-Id ESSO Агент и выберите пункт **Быстрый запуск** (Рисунок 9).

В окне **Выбор приложения** доступны приложения, разрешенные для запуска с помощью Indeed-Id ESSO Агент. Вид окна **Выбор приложения** определяется настройками ESSO-приложений. На

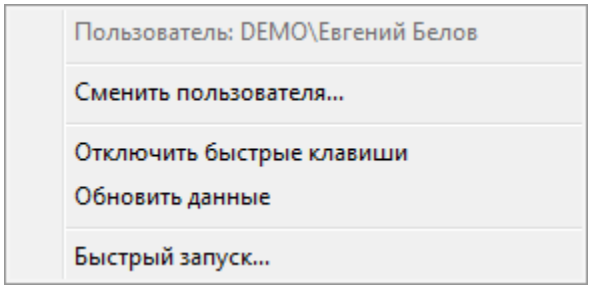

Рисунок 9 – Контекстное меню Indeed-Id ESSO Агент.

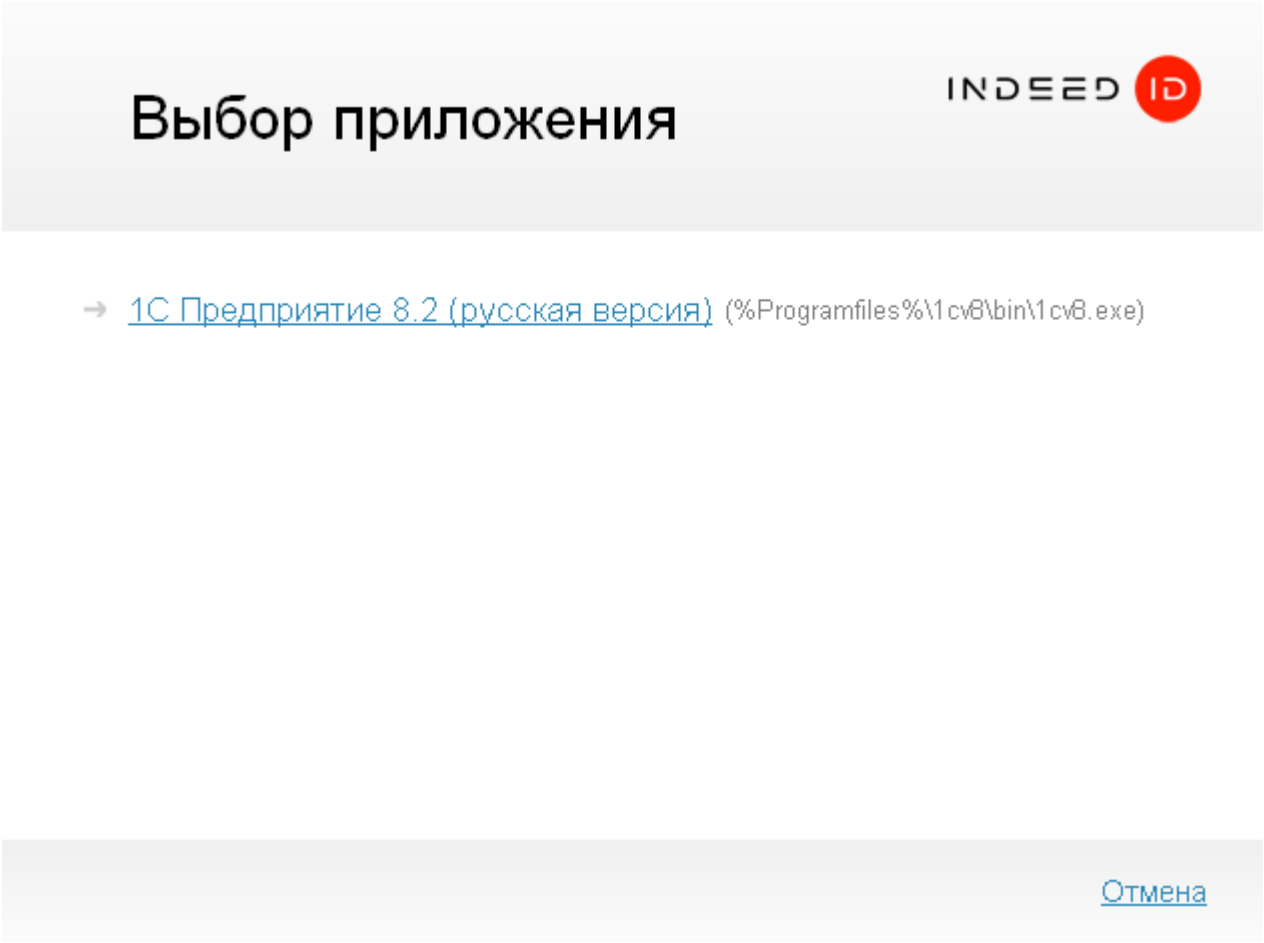

Рисунок 10 – Пример отображения приложения с одним исполняемым файлом.

Если для одного целевого приложения настроено несколько учетных записей SSO, то после выбора приложения потребуется выбрать учетную запись.

Рисунке 10 представлена ситуация, когда у целевого приложения один исполняемый файл.

Если приложение содержит в себе несколько компонентов (например, приложение «1С Предприятие» может содержать в себе приложения «1С:Бухгалтерия», «1С:Управление Торговлей» и т.д.), то исполняемые файлы каждого компонента группируются для удобства выбора в панели быстрого запуска под одним именем. На Рисунке 11 приведен пример группировки нескольких компонентов 1С под одним именем 1С:Предприятие.

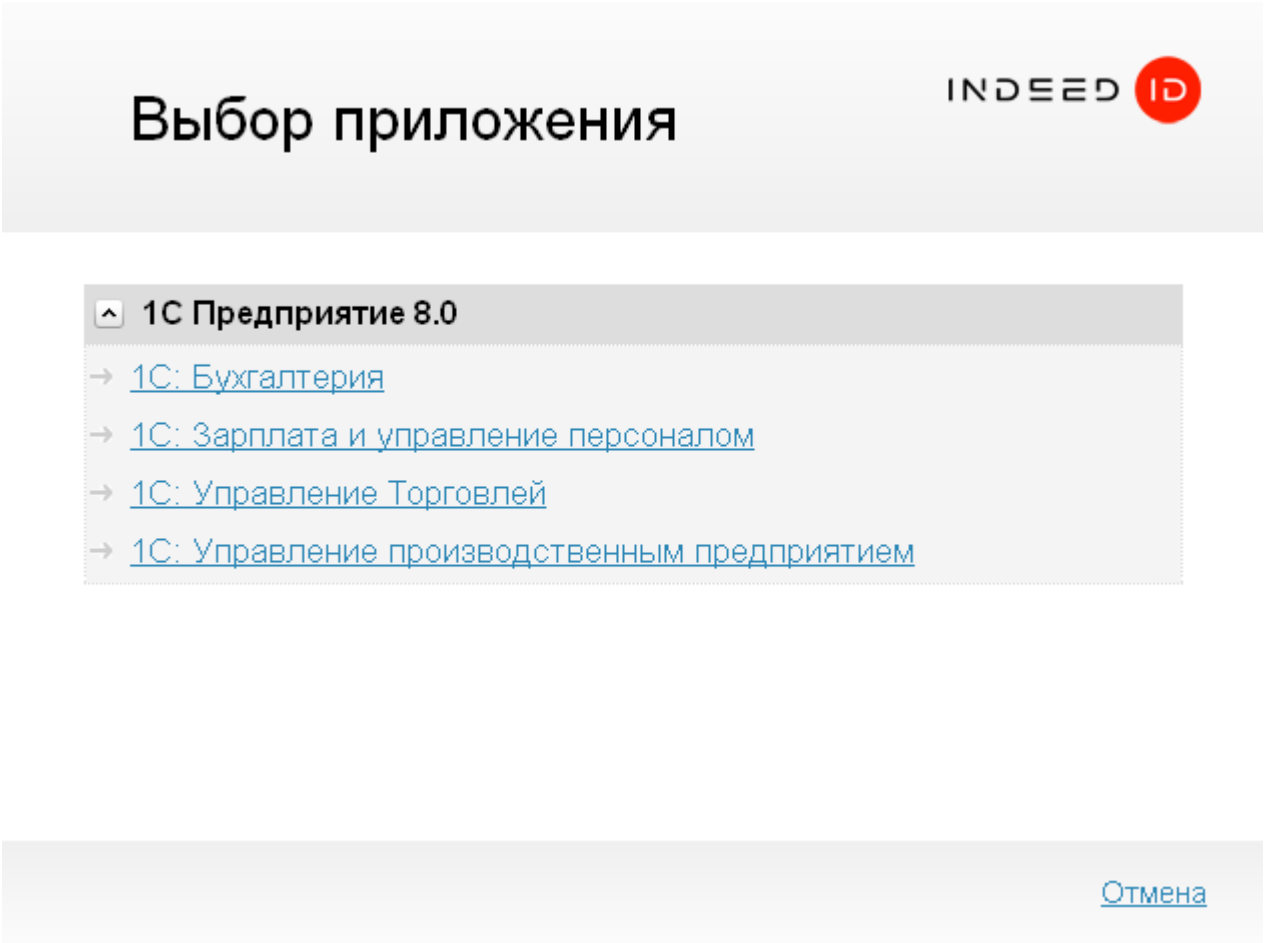

Рисунок 11 – Пример отображения приложения со множеством возможных вариантов запуска.

После выбора приложения потребуется выбрать учетную запись, если их несколько для выбранного приложения (Рисунок 12).

Аутентификация

Для аутентификации в приложении выполните следующие действия:

1. Выберите имя пользователя и способ входа. По умолчанию операционная система предлагает последний использованный способ. Следуйте подсказкам на экране и предоставьте обученный аутентификатор. При наличии нескольких обученных аутентификаторов используйте любой из них.
2. Для выбора аутентификатора нажмите **Сменить способ входа** (Рисунок 13).

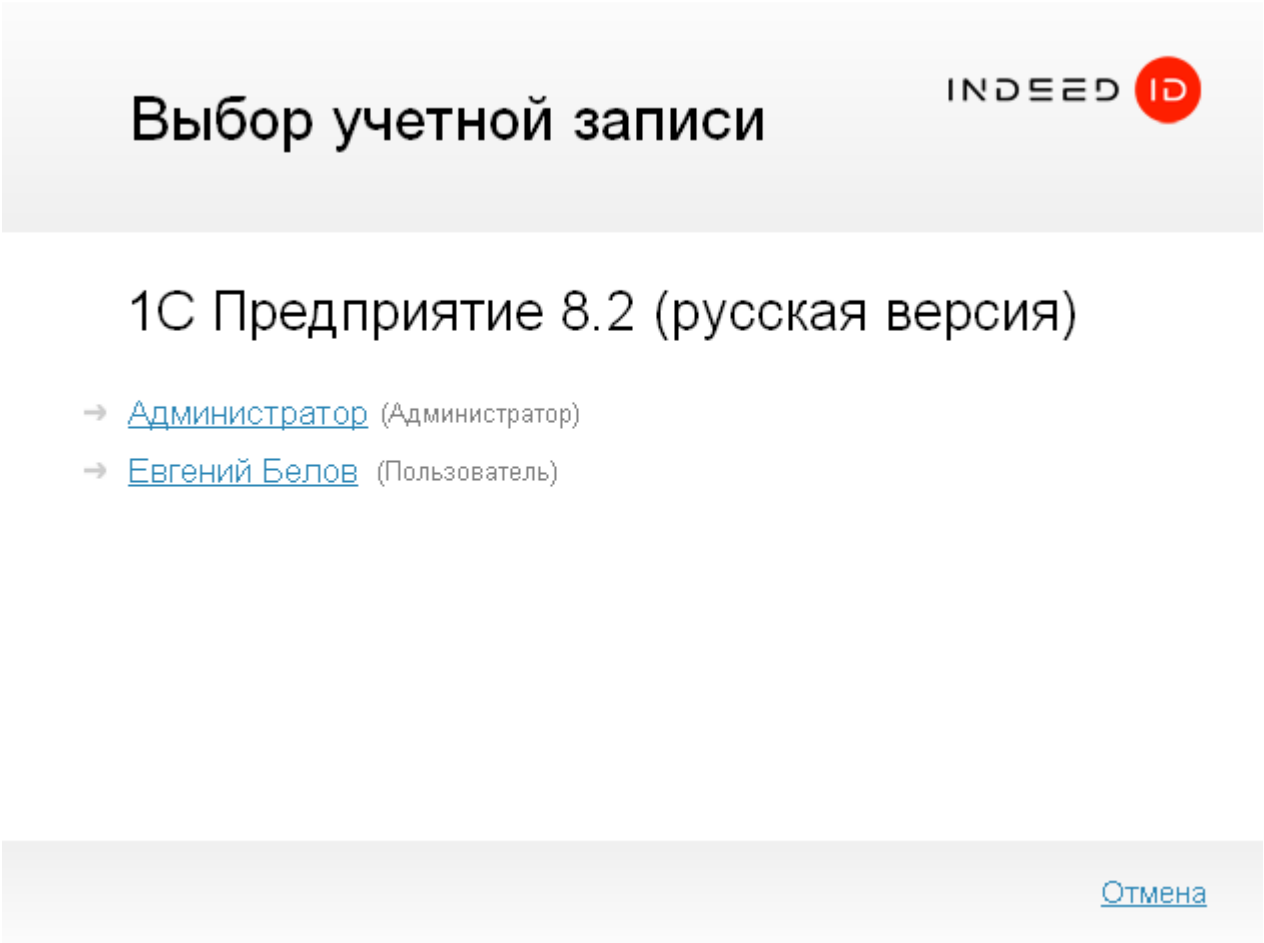

Рисунок 12 – Выбор учетной записи для работы с приложением.

3. После аутентификации отображается окно входа в целевое приложение. В поля «Имя пользователя» и «Пароль» автоматически подставляются данные, указанные при создании учетной записи SSO, и выполняется вход в приложение.
   Помимо автоматической подстановки учетных данных в форму входа приложения поддерживается и ручной ввод логина и пароля. Указанные при первом входе в приложение логин и пароль запоминаются и будут автоматически подставлены при следующем входе. При отмене аутентификации вход в приложение не будет выполнен: текущая форма приложения или само приложение будет закрыто.
4. Если в настройках запуска приложения администратором определен параметр запуска приложения только при помощи Indeed-Id ESSO Агент и настроено требование аутентификации при входе в приложение, то в случае отмены аутентификации отобразится сообщение об ошибке (Рисунок 14).

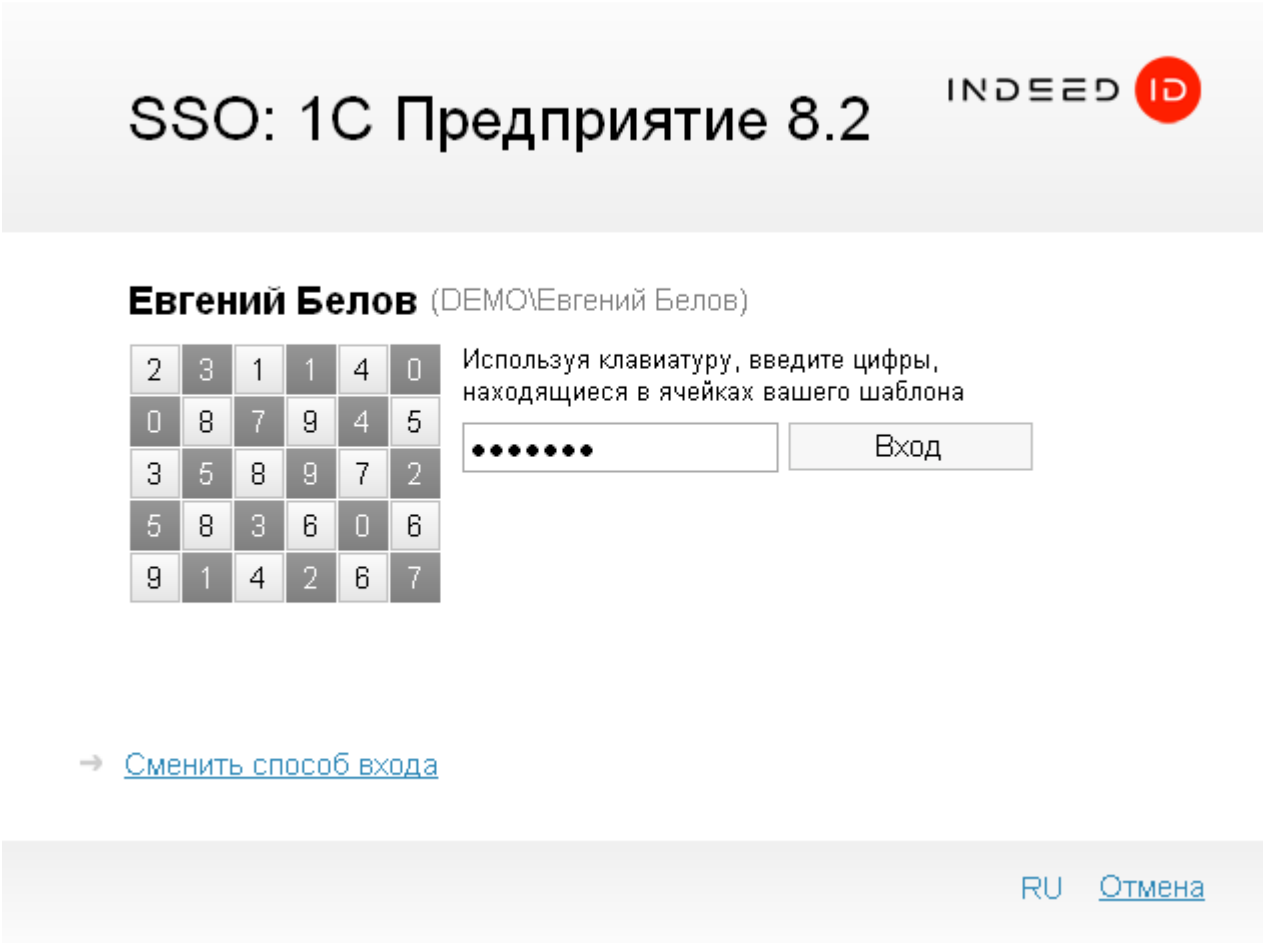

Рисунок 13 – Аутентификация в приложении 1С Предприятие по технологии One Time Matrix.

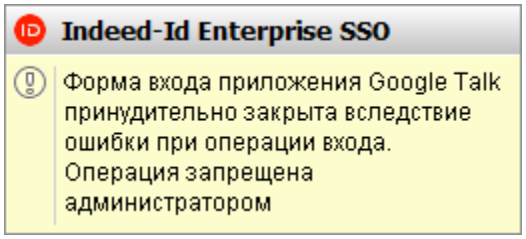

Рисунок 14 – Сообщение Indeed-Id ESSO Агент о закрытии приложения в случае отмены аутентификации.

Доступ к целевым приложениям регулируется административными настройками. Некоторые приложения могут быть запрещены для запуска администратором ESSO. Запрещенные приложения недоступны в окне **Выбор приложения** Indeed-Id ESSO Агент. При попытке запуска запрещенного приложения отображается сообщение об ошибке «A device attached to the system is not functioning» (Рисунок 15):

Смена пользователя

Для изменения пользователя ESSO выполните следующие действия:

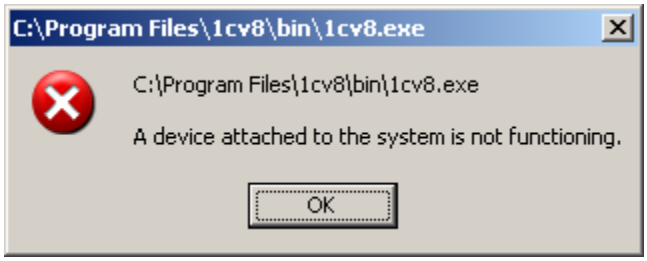

Рисунок 15 – Сообщение Indeed-Id ESSO Агент при попытке запуска приложения из черного списка.

1. Выполните вход в операционную систему и перейдите в контекстное меню Indeed-Id ESSO Агент:
   - Нажмите [**Ctrl**]+[**Alt**]+[**Q**] или откройте приложение Indeed-Id Enterprise SSO Агент двойным щелчком по иконке в области уведомлений Windows.
   - Нажатием правой кнопки мыши на иконку в области уведомлений Windows вызовите контекстное меню приложения Indeed-Id Enterprise SSO Агент и выберите пункт **Сменить пользователя. . .**
2. В окне Вход в SSO выберите пользователя или пункт Автоматическая идентификация, если она включена (Рисунок 16).

Рисунок 16 – Вход в SSO при смене пользователя.

3. Выполните аутентификацию по имеющимся у выбранного пользователя аутентификатору. В случае успешной аутентификации Агент ESSO откроет сессию SSO выбранного пользователя (Рисунок 17):

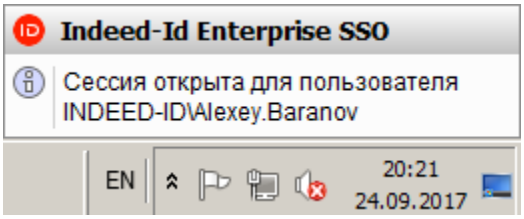

Рисунок 17 – Открытие сессии SSO после смены пользователя.

Управление аутентификаторами

Управление аутентификаторами пользователя осуществляется при помощи приложения **Indeed-Id Управление аутентификаторами**. Приложение позволяет пользователю выполнять следующие действия с аутентификаторами:

- Регистрировать
- Перерегистрировать
- Удалять
- Редактировать комментарий

Перечень действий, которые пользователь может выполнять над аутентификаторами, **задается администратором системы в свойствах пользователя на вкладке Аутентификаторы консоли управления Indeed EMC**.
Подробные сведения по настройке свойств пользователя содержатся в документе *Indeed Enterprise Management Console. Руководство по установке и администрированию.pdf*.

1. Запустите приложение **Indeed-Id Управление аутентификаторами** из меню *Пуск – Все программы – Indeed-Id*. Для работы с приложением Indeed-Id Управление аутентификаторами необходимо выполнить вход в приложение с использованием любого из зарегистрированных аутентификаторов Indeed-Id или по доменному паролю. Если зарегистрированных аутентификаторов нет, то после аутентификации по доменному паролю пользователю будет предложено зарегистрировать аутентификатор.
2. В окне **Аутентификация** (Рисунок 18) выберите свою учетную запись и способ входа (тип аутентификатора). По умолчанию автоматически выбирается последний использованный способ входа. Выполните требуемые действия (в зависимости от выбранного способа входа).

В случае аутентификации по доменному паролю при наличии как минимум одного зарегистрированного аутентификатора Indeed-Id, независимо от настроек, выставленных в свойствах пользователя администратором системы, пользователю будет доступен только просмотр списка зарегистрированных аутентификаторов и проверка каждого из них.
Только пользователи, прошедшие аутентификацию по одному из обученных аутентификаторов Indeed-Id, имеют возможность управлять своими аутентификаторами (в соответствии с настройками, заданными администратором системы для пользователя).

Рисунок 18 – Окно аутентификации в приложении Управление аутентификаторами.

3. После успешной аутентификации отображается окно **Управление аутентификаторами** (Рисунок 19).

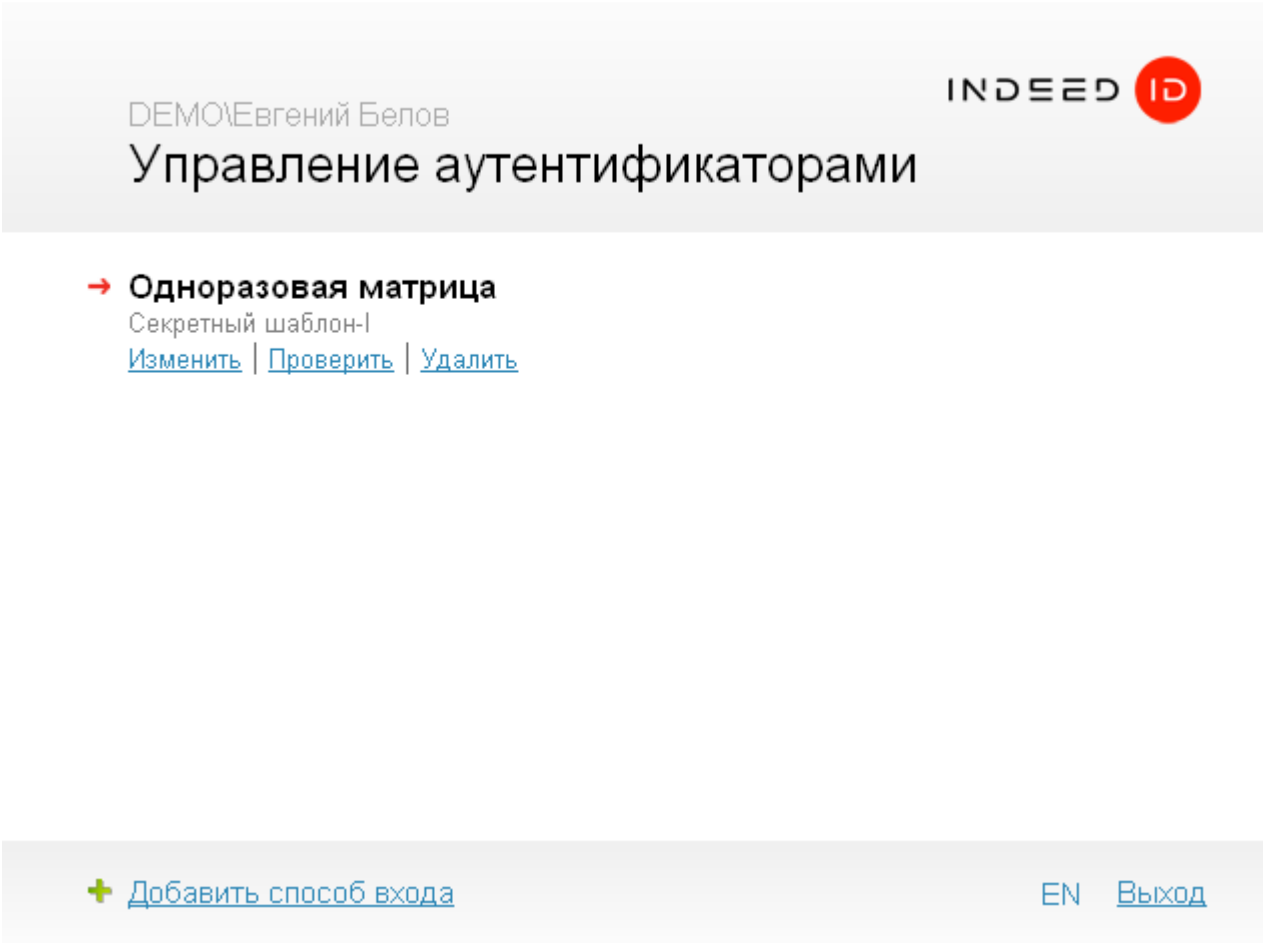

Рисунок 19 – Управление аутентификаторами.

Добавление аутентификатора

Количество аутентификаторов пользователя устанавливается администратором Indeed ESSO. После достижения максимального количества аутентификаторов кнопка **Добавить способ входа** в окне **Управление аутентификаторами** отображаться не будет.
Для добавления аутентификатора выполните следующие действия:

1. В окне **Управление аутентификаторами** нажмите **Добавить способ входа**. Выберите технологию аутентификации (например, «Карта». Рисунок 20).

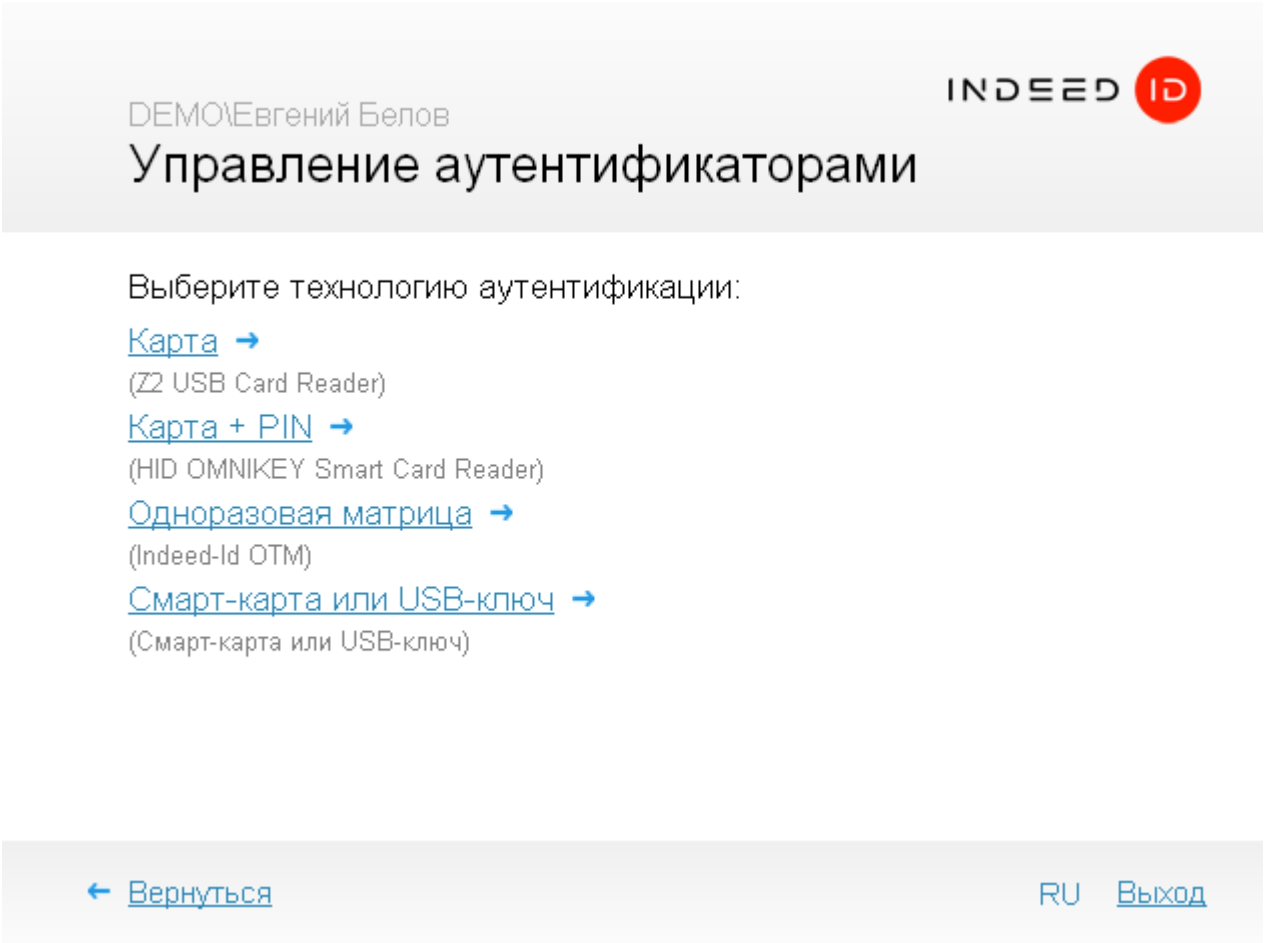

Рисунок 20 – Выбор технологии аутентификации.

2. Следуйте инструкциям по регистрации аутентификатора. Внешний вид окна и текст подсказок зависят от выбранного типа аутентификатора (Рисунок 21).

Рисунок 21 – Регистрация аутентификатора.

3. После успешной регистрации аутентификатора в окне **Управление аутентификаторами** отображается сообщение **Новый аутентификатор успешно обучен** (Рисунок 22).

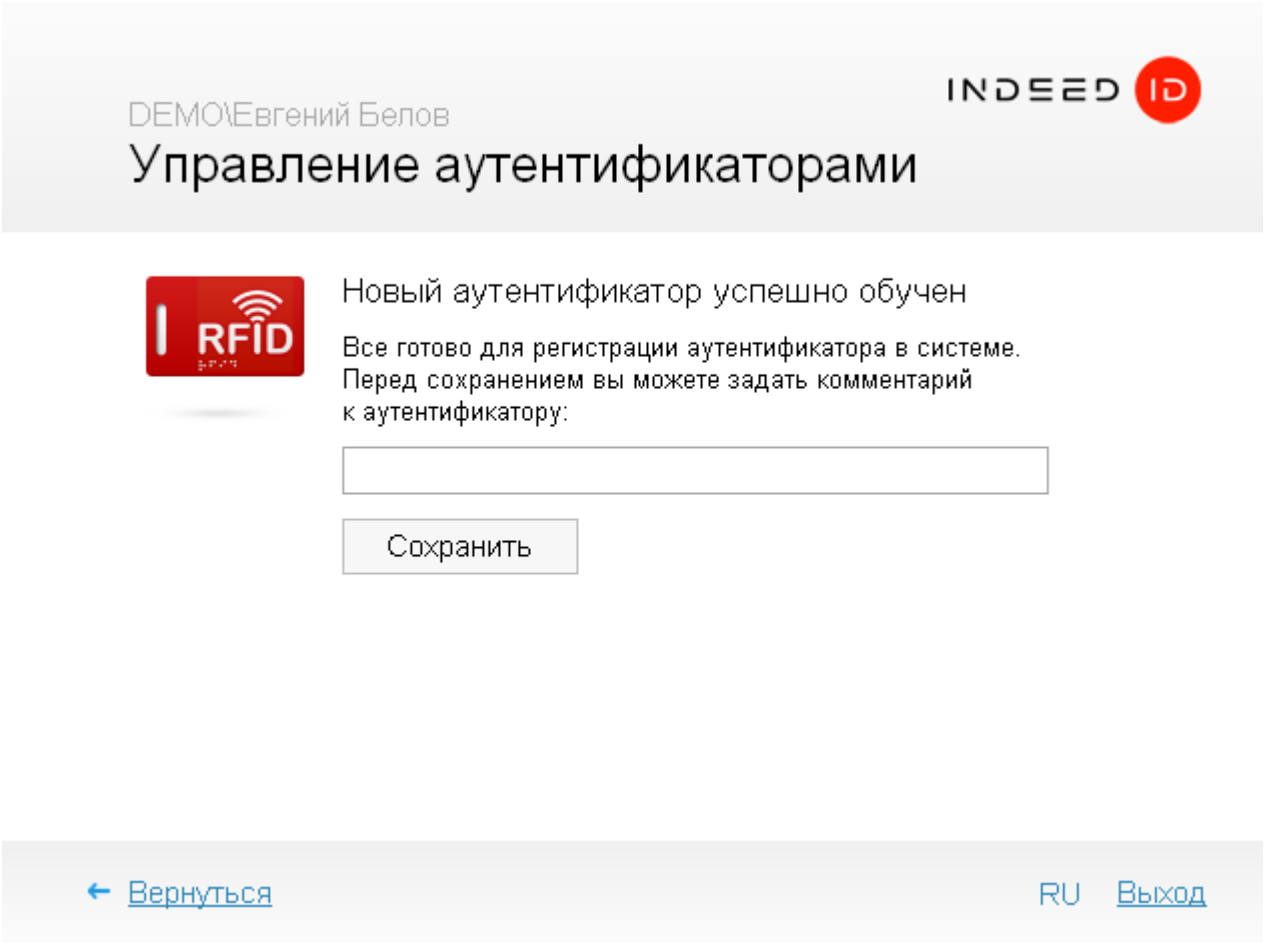

Рисунок 22 – Создание комментария к зарегистрированному аутентификатору.

4. Добавьте произвольный текстовый комментарий к зарегистрированному аутентификатору (если это разрешено администратором Indeed ESSO). Для завершения регистрации аутентификатора нажмите **Сохранить**.

Изменение аутентификатора

Изменять, повторно регистрировать и редактировать комментарий аутентификатора могут только те пользователи, которым перечисленные опции разрешены администратором Indeed ESSO.

Для изменения аутентификатора выполните следующие действия:

1. В окне **Управление аутентификаторами** выберите аутентификатор и нажмите **Изменить** (Рисунок 23).

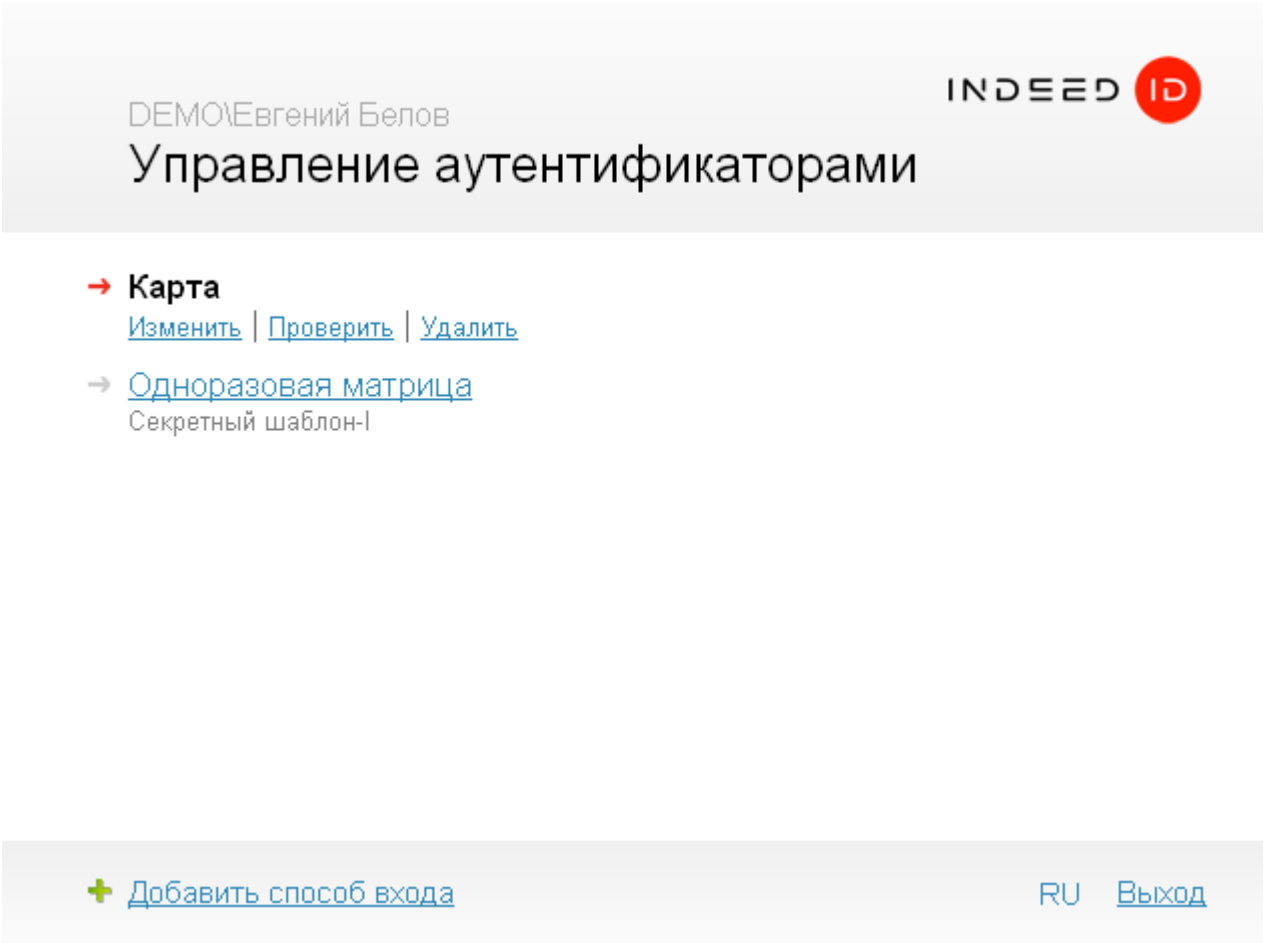

Рисунок 23 – Изменение зарегистрированного аутентификатора.

2. Для изменения комментария к аутентификатору, введите его в соответствующее поле и нажмите **Сохранить** (Рисунок 24).

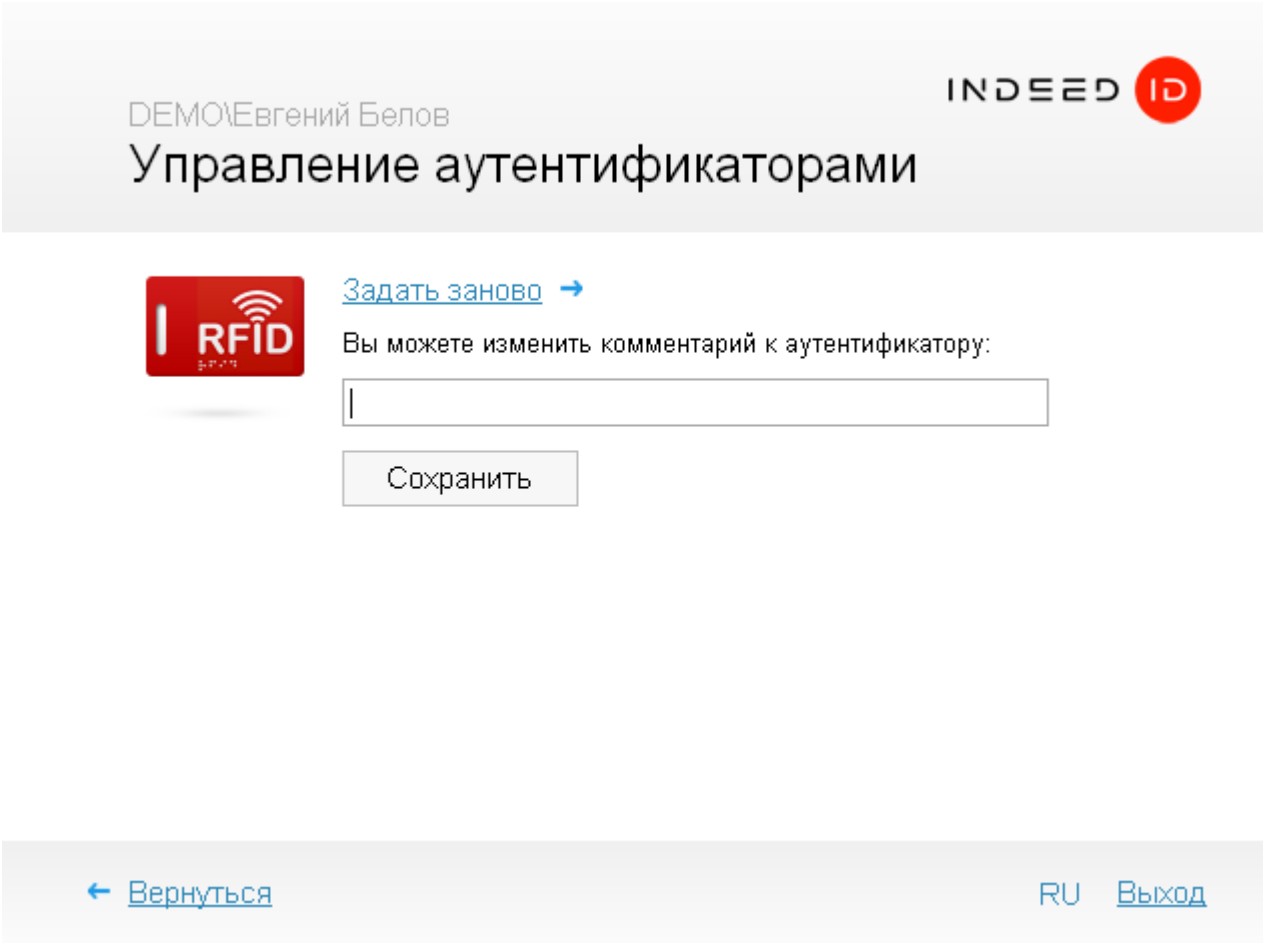

Рисунок 24 – Изменение комментария.

3. Для изменения аутентификатора нажмите **Задать заново**. После этого в окне отобразятся инструкции по регистрации аутентификатора. Внешний вид окна и текст инструкций зависят от выбранного типа аутентификатора. Выполните требуемые действия.
4. После успешной регистрации аутентификатора нажмите **Сохранить**.

Проверка аутентификатора

Для проверки аутентификатора выполните следующие действия:

1. В окне **Управление аутентификаторами** выберите аутентификатор и нажмите **Проверить** (Рисунок 25).

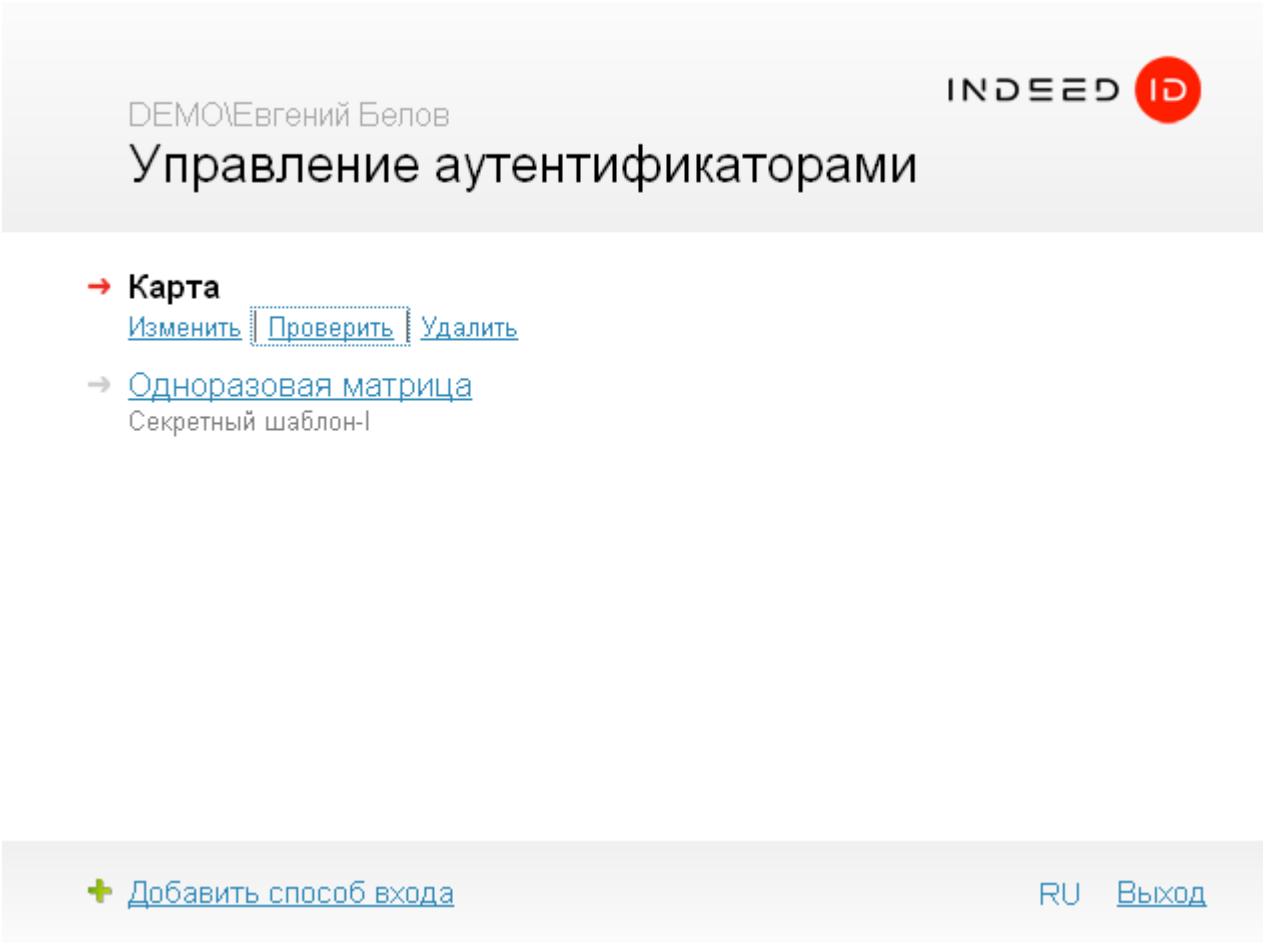

Рисунок 25 – Проверка зарегистрированного аутентификатора.

2. В окне **Управление аутентификаторами** отобразятся инструкции по проверке аутентификатора. Внешний вид окна и текст подсказок зависят от выбранного типа аутентификатора. Выполните требуемые действия.

3. Результаты проверки аутентификатора:
    - Если аутентификаторы совпадают (Рисунок 26):

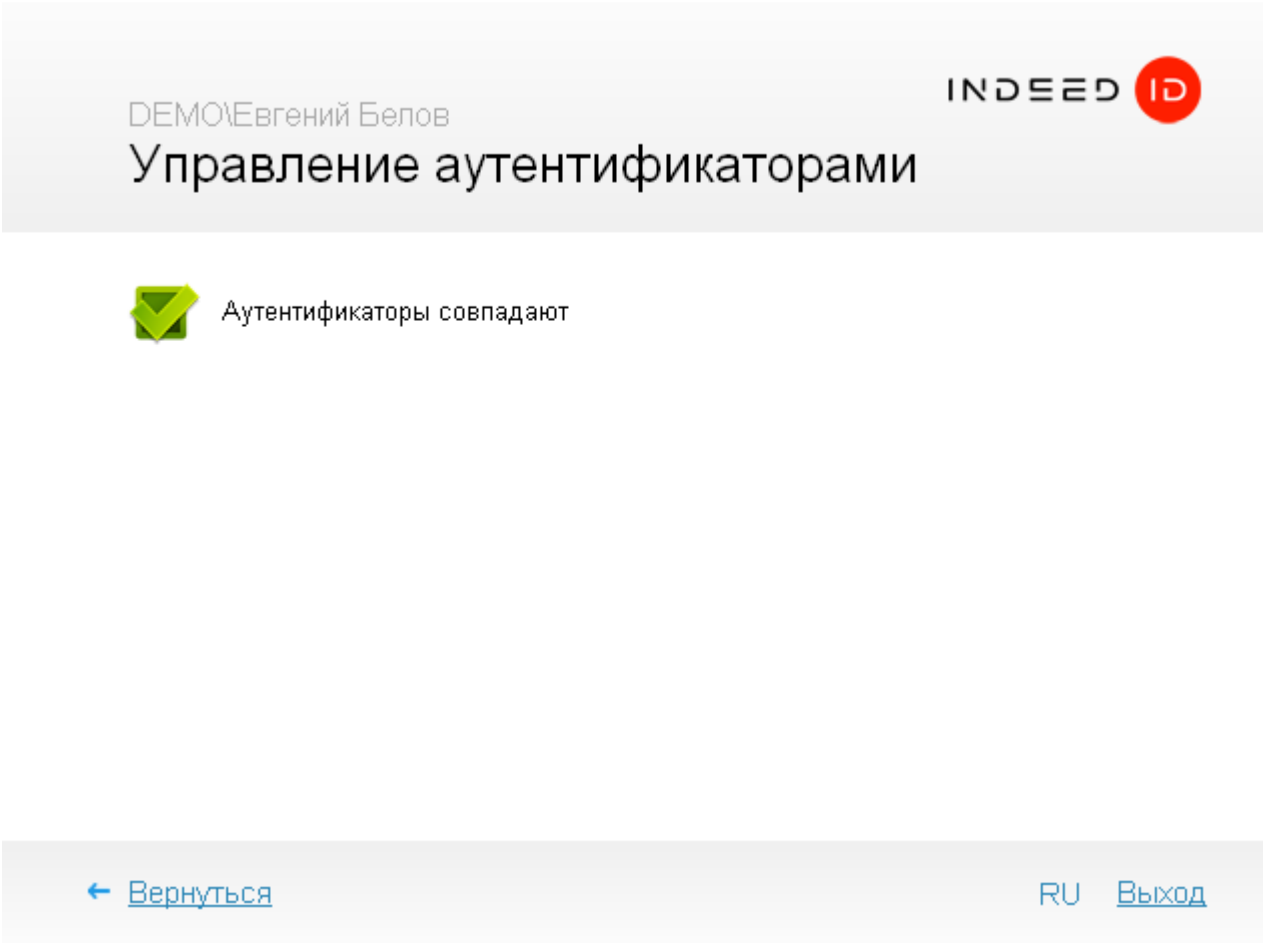

Рисунок 26 – Аутентификаторы совпадают.

- Если аутентификаторы не совпадают (Рисунок 27):

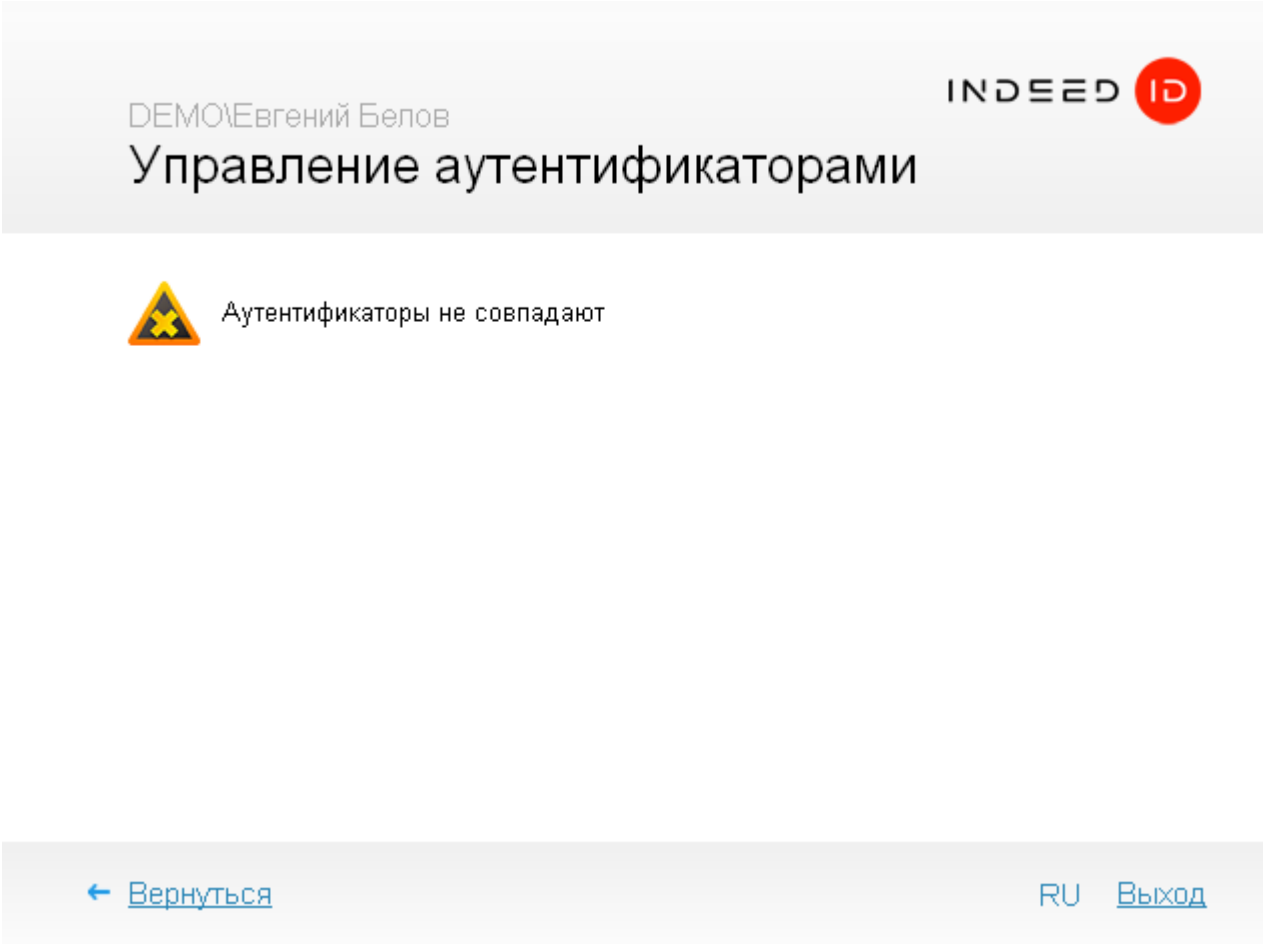

Рисунок 27 – Аутентификаторы не совпадают.

Если аутентификаторы не совпадают, нажмите **Вернуться** и повторите процедуру проверки или заново обучите аутентификатор.

Удаление аутентификатора

Для удаления аутентификатора выполните следующие действия:

- В окне **Управление аутентификаторами** выберите аутентификатор и нажмите **Удалить.** Для подтверждения действия нажмите **Да** (Рисунок 28).

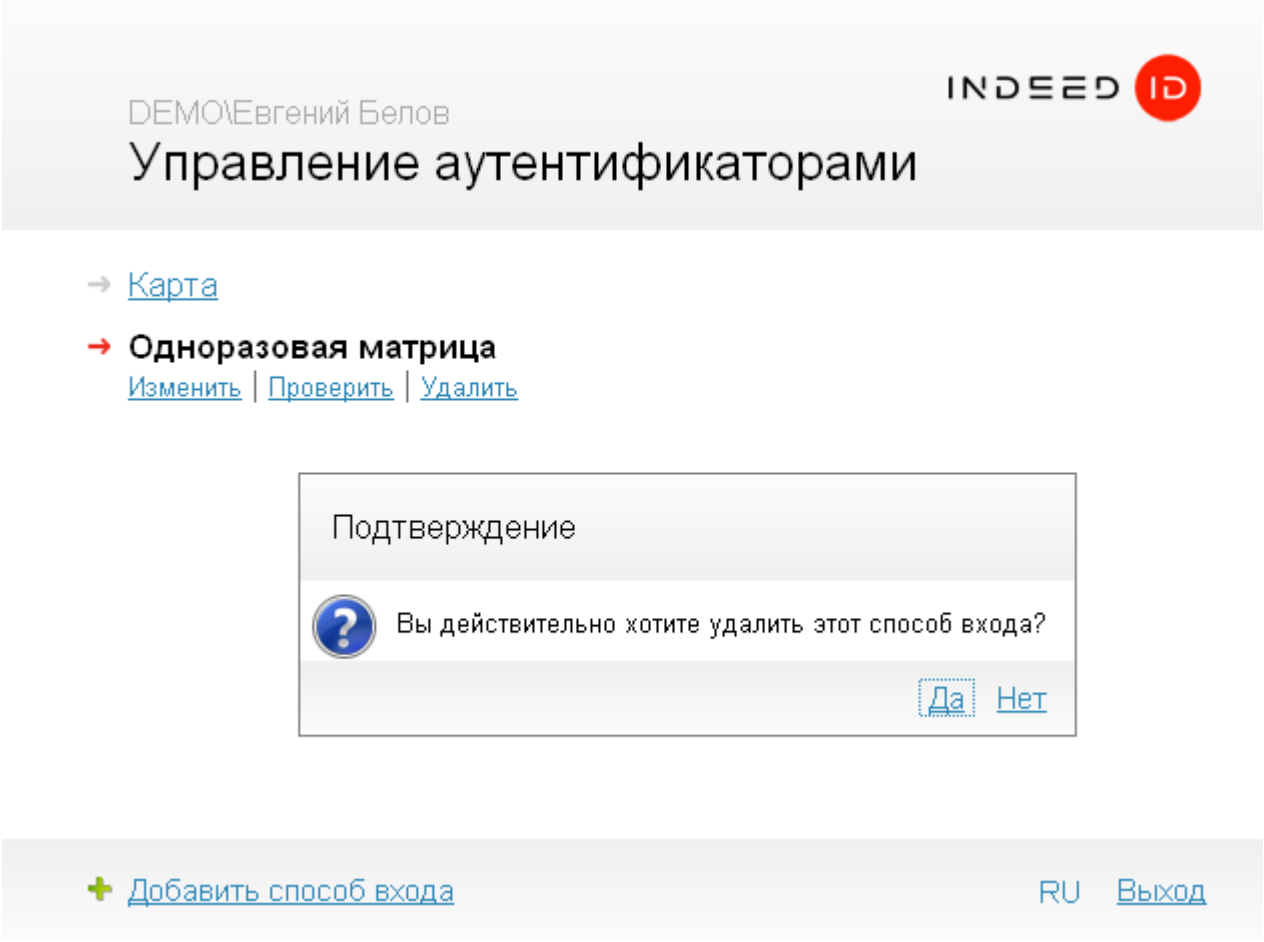

Рисунок 28 – Удаление аутентификатора.

- Если для вашей учетной записи был сгенерирован случайный пароль, при попытке удалить единственный имеющийся аутентификатор появится диалог-предупреждение (Рисунок 29).

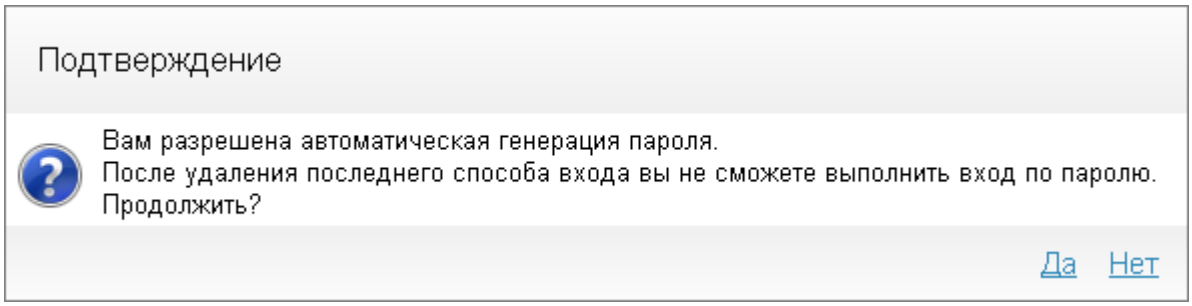

Рисунок 29 – Подтверждение удаления последнего аутентификатора.

Если вы удалили все аутентификаторы и не можете выполнить вход в операционную систему или приложение, обратитесь к администратору.

Управление паролем

Indeed Enterprise Single Sign-On предусматривает регулярную смену пароля в приложениях. Как правило, пароль меняется автоматически. Самостоятельная ручная смена пароля регулируется установками администратора ESSO. Если ручная смена пароля разрешена, при очередной смене пароля новое значение пароля не генерируется автоматически, а запрашивается у пользователя. Поведение при запросе нового пароля у пользователя зависит от типа учетной записи пользователя Enterprise SSO, выбранного администратором ESSO: Если администратором настроена ручная смена пароля пользователем, то при смене пароля отобразится следующее окно (Рисунок 30).

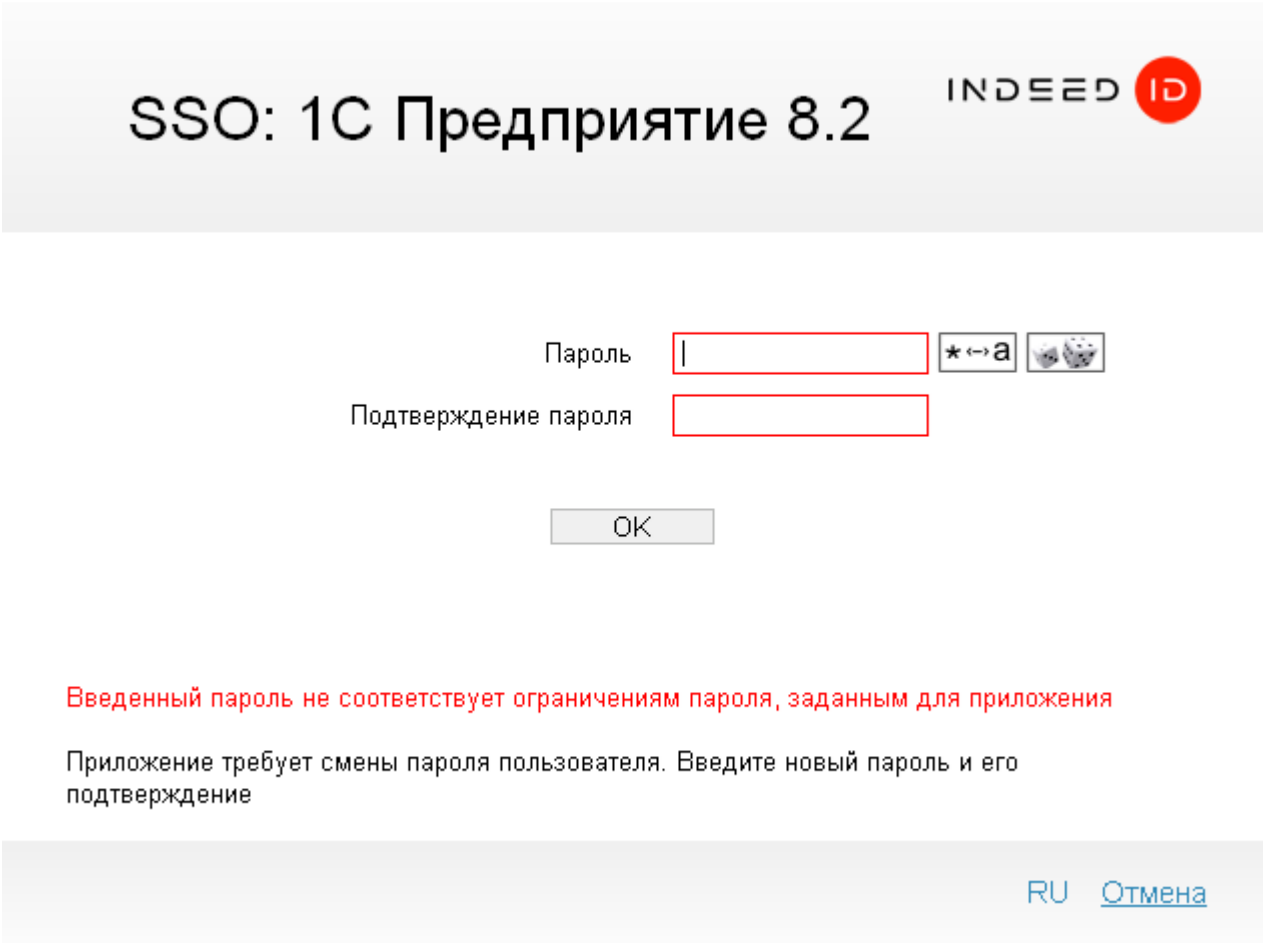

Рисунок 30 – Изменение пароля приложения пользователем.

Введите новый пароль и его подтверждение.

- Режим ввода пароля (скрытый пароль/открытый ввод символов) регулируется нажатием кнопки  (**Открыть пароль**).
- При нажатии кнопки  (**Генерировать случайный пароль**) выполняется автоматическая генерация пароля в соответствии с установленными для данного приложения ограничениями. Сгенерированный пароль автоматически вставляется в поле **Пароль**, при этом включается функция **Открыть пароль** и очищается поле **Подтверждение пароля**.

При вводе нового пароля в стандартном режиме выполняется проверка пароля на соответствие критериям сложности, установленным для данного приложения. В случае несоответствия пароля критериям сложности отображается сообщение об ошибке. Если учетная запись Enterprise SSO относится к типу **Учетных данных Active Directory**, при смене пароля отображается следующее сообщение (Рисунок 31):

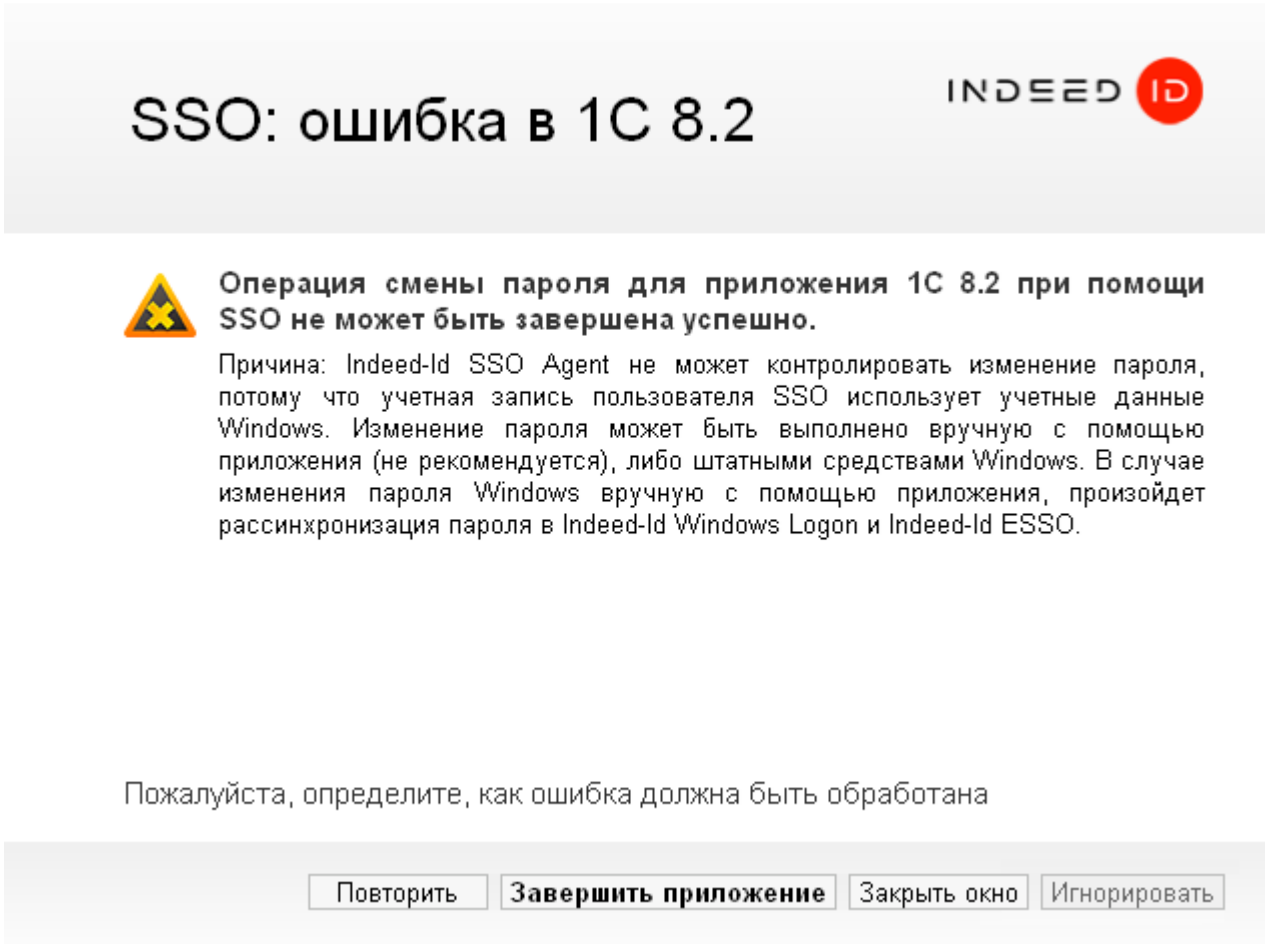

Рисунок 31 – Ошибка смены пароля.

Команды Indeed-Id ESSO Агент

В контекстном меню, которое открывается правым щелчком по иконке приложения Indeed-Id ESSO Агент в панели уведомлений Windows, доступны следующие команды:

Сменить пользователя – выбрать другую учетную запись для получения доступа в приложение. При выборе команды отображается окно Вход в SSO со списком доступных учетных записей и возможностью выбрать способ входа. По умолчанию используется способ, при помощи которого выполнялся последний вход пользователя.

Отключить быстрые клавиши – отключение использование комбинаций клавиш:

[Ctrl]+[Alt]+[Q] - вызов окна быстрого запуска

[Ctrl]+[Alt]+[U] - обновление данных ESSO

[Ctrl]+[Alt]+[R] - принудительная обработка формы приложения («рематчинг»)

По умолчанию все комбинации включены.

Обновить данные – загрузка изменений профиля SSO. Примеры сообщений приведены на Рисунках 32, 33 и 34.

Рисунок 32 – Обновление данных ESSO.

Рисунок 33 – Новые данные ESSO получены.

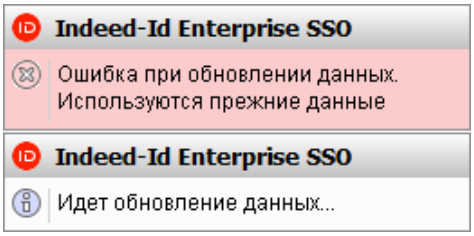

Рисунок 34 – Ошибка обновления данных.

Быстрый запуск – выполняется при выборе соответствующего пункта в контекстном меню Indeed-Id ESSO Агент или нажатии комбинации [Ctrl]+[Alt]+[Q] и предоставляет доступ к списку приложений, разрешенных для запуска (открывается окно **Выбор приложения**).

Приложение не отображается в списке, если Indeed-Id ESSO Агент не может найти его исполняемый файл на рабочей станции пользователя.

Обработка ошибок

При возникновении ошибок во время работы (например, ошибка заполнения формы) Indeed-Id ESSO Агент предоставляет возможность выбора действия для обработки ошибки. В таких случаях отображается окно Обработка ошибки (Рисунок 35).

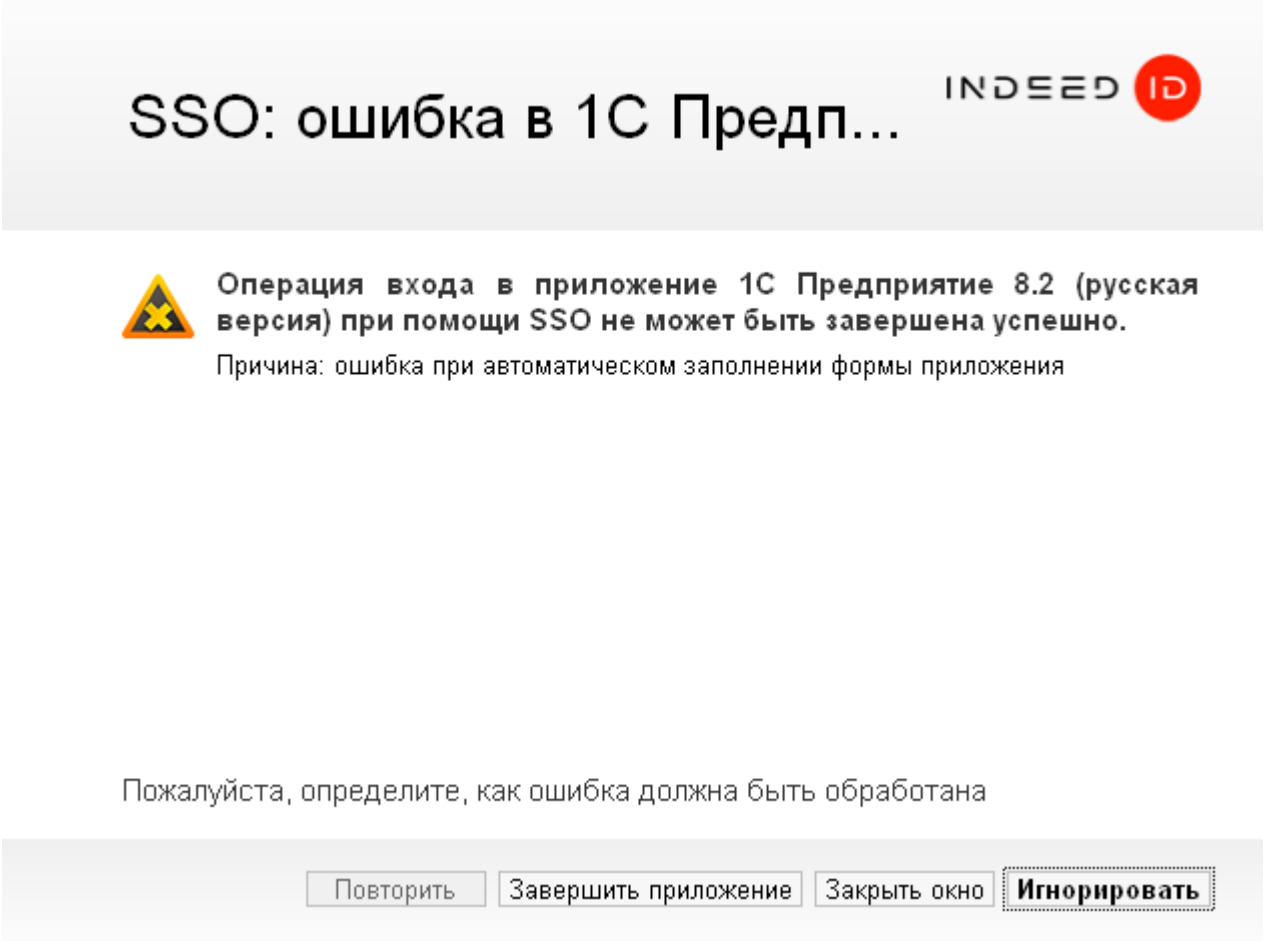

Рисунок 35 – Обработка ошибки Indeed-Id ESSO Агент.

В окне **Обработка ошибки** предлагаются варианты действий (после выбора действия окно закроется автоматически):

Повторить – операция, в ходе которой возникла ошибка, будет выполнена повторно.

Завершить приложение – приложение, при работе с которым возникла ошибка, будет завершено. Не сохраненные данные будут потеряны.

Закрыть окно – будет закрыто текущее окно или форма приложения. При закрытии главного окна приложение может быть завершено.

Игнорировать – не будет предпринято никаких действий.

Сбор программных логов

Сбор логов приложений

Наличие программных логов позволяет специалистам службы поддержки определить причины возможных проблемных ситуаций и принять меры к их устранению. Сбор программных логов осуществляется утилитой GetLog, поставляемой в составе дистрибутива Indeed EA/ESSO. Для получения подробной информации обратитесь к документу *Indeed-Id GetLog. Руководство по эксплуатации.pdf*.

Сбор логов web-сервисов

1. Перейдите в каталог приложения **emc** (%SystemDrive%\inetpub\wwwroot\emc\Config).
2. Откройте файл **nlog.config** в текстовом редакторе, например, в Блокнот, запущенном от имени администратора, и измените параметр enabled="false" на "true" в секции logger name:

```
<logger name="*" writeTo="f1" enabled="true" />
```

3. Сохраните изменения в файле.
4. Воспроизведите сценарий, логи которого необходимо получить.
5. Перейдите в каталог logs, расположенный в каталоге %SystemDrive%\inetpub\wwwroot\emc
6. Пришлите каталог logs со всем его содержимым на адрес **support@indeed-id.com** с описанием воспроизведения ошибки.
7. Для отключения логирования измените значение параметра enabled с "true" на "false" и сохраните изменения в файле.

Часто задаваемые вопросы

Ознакомьтесь со списком часто задаваемых вопросов и ответов на них в **Базе знаний**:

- Indeed Enterprise Authentication
- Indeed Enterprise Single Sign-On