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 SMS OTP Provider

Руководство по установке и эксплуатации

версия 1.6.2

Содержание

Введение

Приветствуем вас и благодарим за приобретение программных продуктов компании Indeed ID. Это руководство поможет вам ознакомиться с принципом работы компонента **Indeed-Id SMS OTP Provider**, параметрами его установки и настройки.

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 компоненте Indeed-Id SMS OTP Provider

Компонент Indeed-Id SMS OTP Provider предназначен для аутентификации пользователей с применением технологии одноразовых паролей, доставляемых пользователям в коротких текстовых сообщениях (SMS) и совместного использования с продуктами Indeed Enterprise Authentication и Indeed Enterprise Single Sign-On. Одноразовый пароль представляет собой набор случайных символов (цифр, латинских букв и спецсимволов). Генерация пароля происходит на сервере Indeed EA (ESSO) по запросу пользователя, затем пароль передается на сервис рассылки SMS, который пересылает его пользователю в виде текстового сообщения. Передача SMS происходит по протоколу SMPP (англ. *Short message peer-to-peer protocol*).

Indeed-Id SMS OTP Provider может быть дополнен PIN-кодом (Indeed-Id SMS OTP Provider with PIN). В этом случае для аутентификации пользователю необходимо будет помимо одноразового пароля ввести известный ему PIN-код. Получить доступ по одному лишь одноразовому паролю или PIN-коду невозможно.

Для использования Indeed-Id SMS OTP Provider необходимо наличие сервера отправки текстовых сообщений. Для обмена данных с сервером отправки сообщений рекомендуется обеспечить защищенное соединение. Данный сервер должен быть доступен с каждого сервера Indeed EA (ESSO), на котором предполагается установка Indeed-Id SMS OTP Provider.
Аутентификация пользователей с использованием Indeed-Id SMS OTP Provider возможна только при наличии связи клиентской рабочей станции с сервером Indeed EA (ESSO). Аутентификация по кэшированному аутентификатору с использованием Indeed-Id SMS OTP Provider не поддерживается.

Установка Indeed-Id SMS OTP Provider

Установка Indeed-Id SMS OTP Provider выполняется на всех серверах Indeed-Id и затем на рабочих станциях пользователей[1]. Для установки компонента потребуется минимум 10Мб свободного места на жестком диске компьютера.

Для установки Indeed-Id SMS OTP Provider, пользователь, от имени которого выполняется установка, должен обладать правами администратора (быть членом локальной группы «Администраторы»).

Для развертывания Indeed-Id SMS OTP Provider 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*.

Для установки Indeed-Id SMS OTP Provider выполните следующие действия:

1. Запустите файл IndeedID.SMSOTP.Provider.msi[2] из дистрибутива провайдера и выполните установку, следуя указаниям мастера.
2. После завершения установки может потребоваться перезагрузка системы. Если программа установки предлагает выполнить перезагрузку, подтвердите данное действие.
3. Удаление/Восстановление продукта осуществляется стандартным для поддерживаемых ОС способом, через меню Панель управления.

[1] Если предполагается использовать Indeed-Id SMS OTP Provider совместно с Indeed NPS RADIUS Extension, то устанавливать провайдер на клиентские рабочие станции не требуется

[2] IndeedID.SMSOTP.PIN.Provider.msi если необходимо установить версию провайдера с PIN-кодом.

Настройка параметров аутентификации

Изменение параметров работы провайдера осуществляется через механизм групповых политик Active Directory.

Перед настройкой групповой политики необходимо добавить в список административных шаблонов шаблоны политик Indeed-Id. Файлы шаблонов политик входят в состав дистрибутива провайдера и расположены в каталоге Misc.
Для получения подробной информации обратитесь к документу *Indeed-Id Admin Pack. Руководство по установке и использованию.pdf*.

Группа политик SMS OTP определяет следующие параметры провайдера:

- Минимальная длина PIN-кода[3]
- Сервис отправки SMS
- Параметры SMPP
- Настройки генерации одноразового пароля
- Настройки одновременного подключения к серверу SMPP

Сервис отправки SMS
Политика применяется к серверам Indeed EA (ESSO) и определяет следующие настройки для сервера отправки SMS:

- URL(IP-адрес) - адрес подключения к серверу;
- Порт - порт подключения к серверу;
- SystemId (Логин) - имя учетной записи для подключению к серверу;
- Пароль - пароль учетной записи для подключения к серверу;

Пароль может быть задан как в явном, так и в зашифрованном виде. Для шифрования пароля необходимо использовать утилиту **IndeedID.SMSOTP.Password.Encryptor.exe**, входящую в состав дистрибутива провайдера.

- SystemType - поле PDU операции BIND_TRANSCEIVER протокола SMPP;
- Отправитель - имя отправителя, которое будет отображаться при получении SMS;
- Дополнительный текст перед OTP - произвольный текст сообщения, предшествующий одноразовому паролю;
- Время ожидания статуса SMS - время ожидания получения статуса отправленного SMS с сервера;
- PDU со статусом SMS - PDU, в котором сервер присылает статус отправленного сообщения;

[3]Только для Indeed-Id SMS OTP Provider with PIN.

Не задан (Not Configured) или *Отключен (Disabled)*
Обращение к серверу отправки сообщений происходить не будет.

Включен (Enabled)
При обращении к серверу отправки сообщений будут использованы заданные в политике параметры. Пример настроенной политики приведен на Рисунке 1.

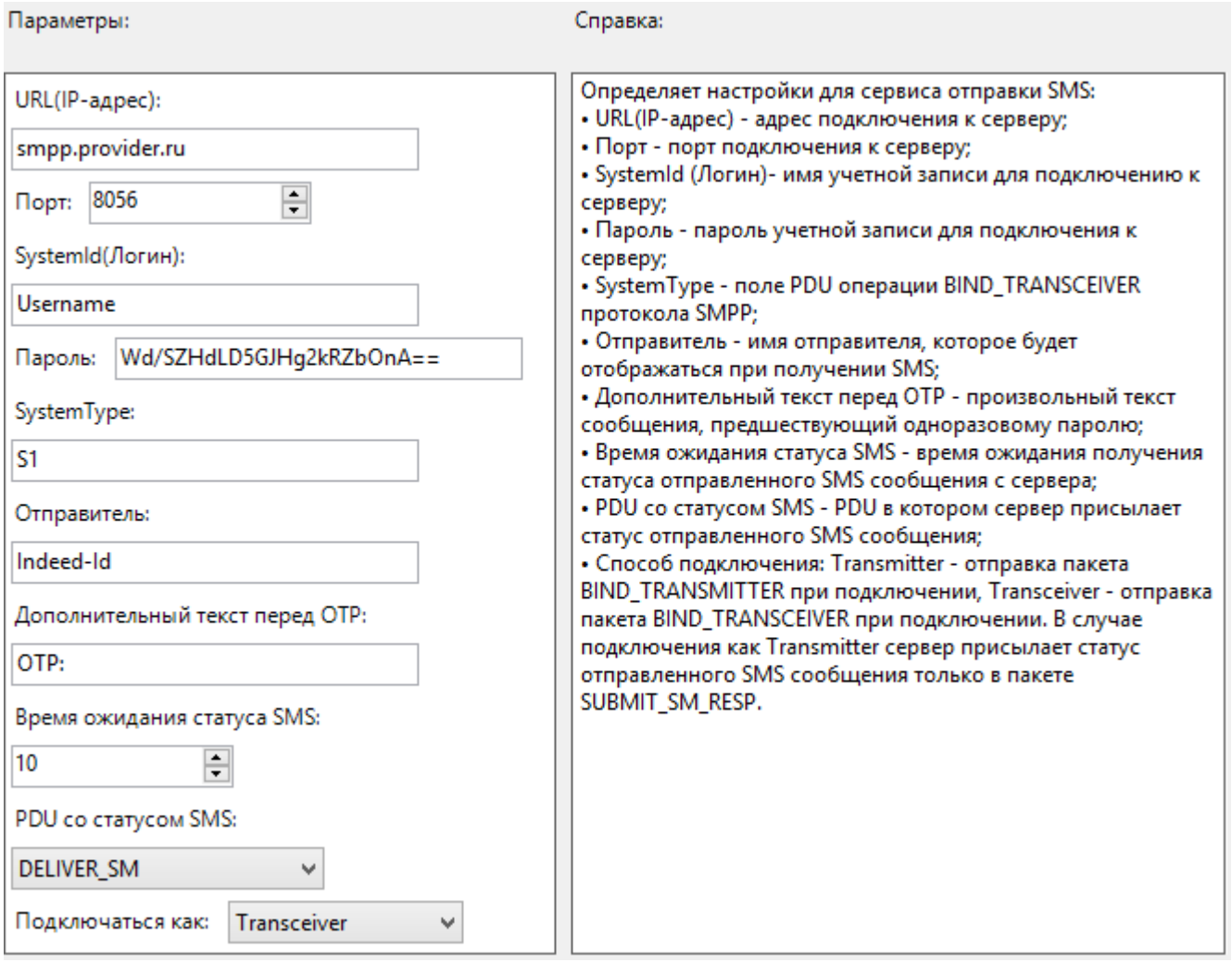

Рисунок 1 – Значения политики "Сервис отправки SMS".

Допустимые значения для каждого пункта политики **Сервис отправки SMS** зависят от используемого сервера отправки SMS.

Параметры SMPP
Политика применяется к серверам Indeed EA (ESSO) и определяет следующие поля PDU операции SUBMIT_SM протокола SMPP:

- **source_addr_ton** - Тип номера (Type of Number) для исходного адреса
- **source_addr_npi** - Индикатор схемы присвоения номеров (Numbering Plan Indicator) для исходного адреса
- **dest_addr_ton** - Тип номера (Type of Number) для адресата
- **dest_addr_npi** - Индикатор схемы присвоения номеров (Numbering Plan Indicator) для адресата
- **esm_class** - Указывает Message Mode & Message Type
- **registered_delivery** - Индикатор для того, чтобы обозначить, что запрашивается расписка о получении SMSC или подтверждение SME
- **data_coding** - Определяет схему кодировки пользовательских данных короткого сообщения

Не задан (Not Configured) или *Отключен (Disabled)*
Передача случайного PIN-кода на сервер отправки сообщений осуществляться не будет.

Включен (Enabled)
Случайный PIN-код будет передан на сервер отправки SMS в соответствии с определенными в политике параметрами. Пример настроенной политики приведен на Рисунке 2.

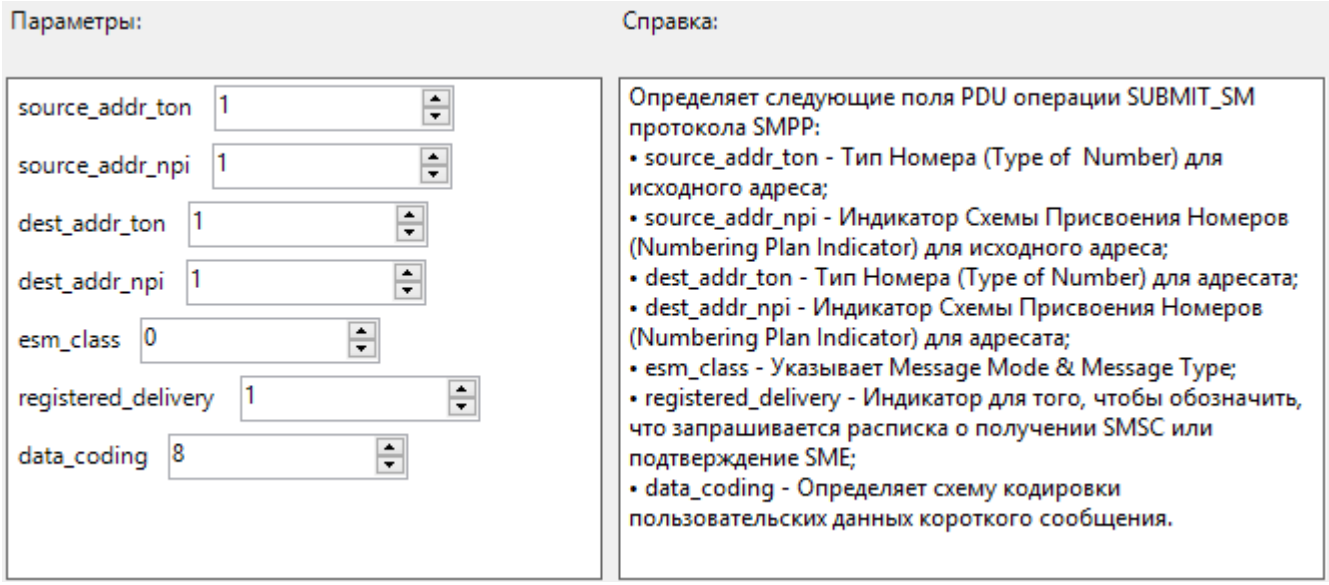

Рисунок 2 – Значения политики "Параметры SMPP".

Допустимые значения для каждого пункта политики **Параметры SMPP** зависят от используемого сервера отправки SMS.

Настройки генерации одноразового пароля
Политика применяется к серверам Indeed EA и позволяет задать длину и вхождение групп символов при генерации одноразового пароля.

Не задан (Not Configured) или *Отключен (Disabled)*
Если политика не задана или отключена, то пароль будет состоять из цифр и иметь длину 6 символов.

Включен (Enabled)
Одноразовый пароль будет генерироваться согласно заданным в политике правилам. Если политика включена, но не определена ни одна группа символов, то пароль будет состоять только из цифр (длина пароля по умолчанию – 6 символов). Пример настроенной политики приведен на Рисунке 3.

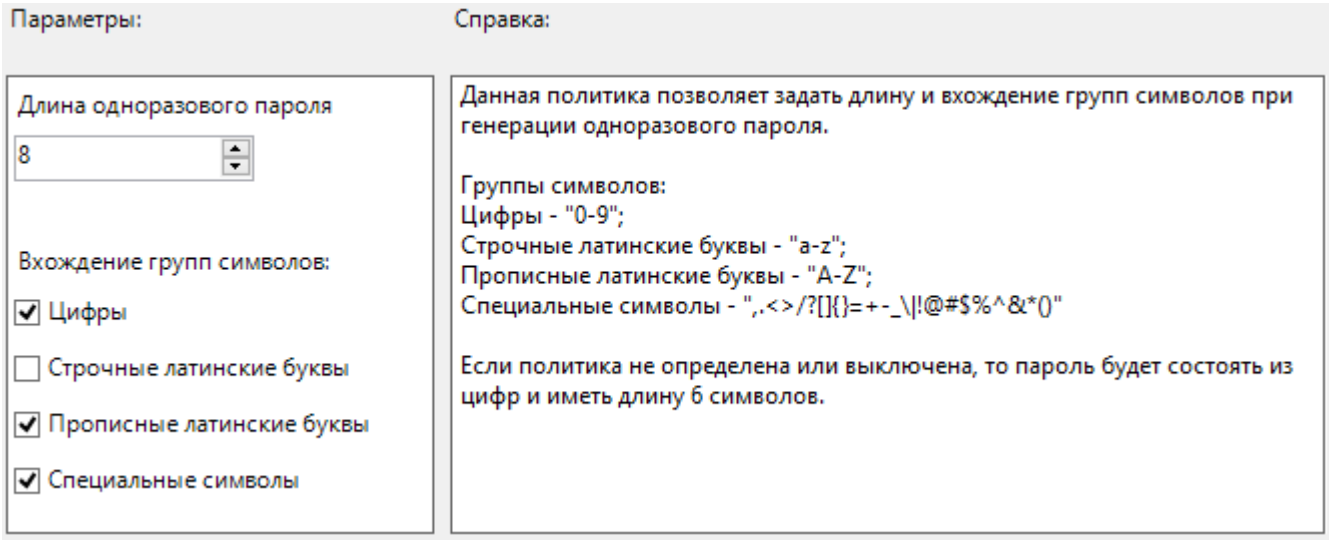

Рисунок 3 – Значения политики "Настройки генерации одноразового пароля.

Минимальная длина PIN-кода
Политика применяется к рабочим станциям пользователей, использующих Indeed-Id SMS OTP Provider with PIN и задает минимальную длину PIN-кода.

Не задан (Not Configured) или *Отключен (Disabled)*
Минимальная длина PIN-кода соответствует значению по умолчанию (4 символа).

Включен (Enabled)
Минимальная длина PIN-кода соответствует заданному в политике значению. Допустимый диапазон от 4 до 25 символов.

Настройки одновременного подключения к серверу SMPP
Политика применяется к серверам Indeed EA (ESSO) и определяет порядок обработки запросов к серверу SMPP. Включение политики может быть необходимо, в случае если сервер SMPP не поддерживает несколько подключений от одного пользователя (учетной записи, указанной в политике Сервис отправки SMS) одновременно.

Не задан (Not Configured) или *Отключен (Disabled)*
Подключение к серверу SMPP и запросы на отправку сообщений будут происходить параллельно.

Включен (Enabled)
Подключение к серверу SMPP и запросы на отправку сообщений будут происходить последовательно.

Для того чтобы изменения в настройках политик вступили в силу, необходимо выполнить обновление групповой политики. Для немедленного обновления групповой политики используйте команду **gpupdate /force**.

Работа с Indeed-Id SMS OTP Provider

Регистрация аутентификатора

Аутентификатор – набор данных, создаваемый для каждого пользователя системы Indeed-Id, необходимый, для прохождения процедуры аутентификации. Каждый новый пользователь системы Indeed-Id должен пройти процедуру регистрации одного или нескольких аутентификаторов.

Регистрация аутентификатора осуществляется после установки на рабочую станцию пользователя необходимых компонентов системы Indeed EA(ESSO): Indeed-Id Windows Logon или Indeed-Id ESSO Агент (в зависимости от используемой конфигурации системы) и провайдера Indeed-Id SMS OTP Provider. Пользователь выполняет вход в систему по доменному паролю и, следуя указаниям приложения **Indeed-Id Управление аутентификаторами**, регистрирует аутентификатор.

Для успешной регистрации аутентификатора необходимо, чтобы пользователю, от имени которого осуществляется регистрация, было разрешено использовать технологию аутентификации Indeed-Id. Соответствующая настройка **выполняется администратором системы в свойствах пользователя на вкладке *Настройки* в консоли управления Indeed EMC**.
Подробные сведения по настройке свойств пользователя содержатся в документе *Indeed Enterprise Management Console. Руководство по установке и администрированию.pdf*.

Если аутентификатор не был зарегистрирован при первом входе пользователя в систему, регистрацию можно выполнить в любой удобный момент, запустив приложение **Indeed-Id Управление аутентификаторами** из меню *Пуск – Все программы – Indeed-Id*.

Для регистрации аутентификатора необходимо войти в систему по доменному паролю и выполнить следующие действия: В окне **Управление аутентификаторами** нажмите **Продолжить** (Рисунок 4).

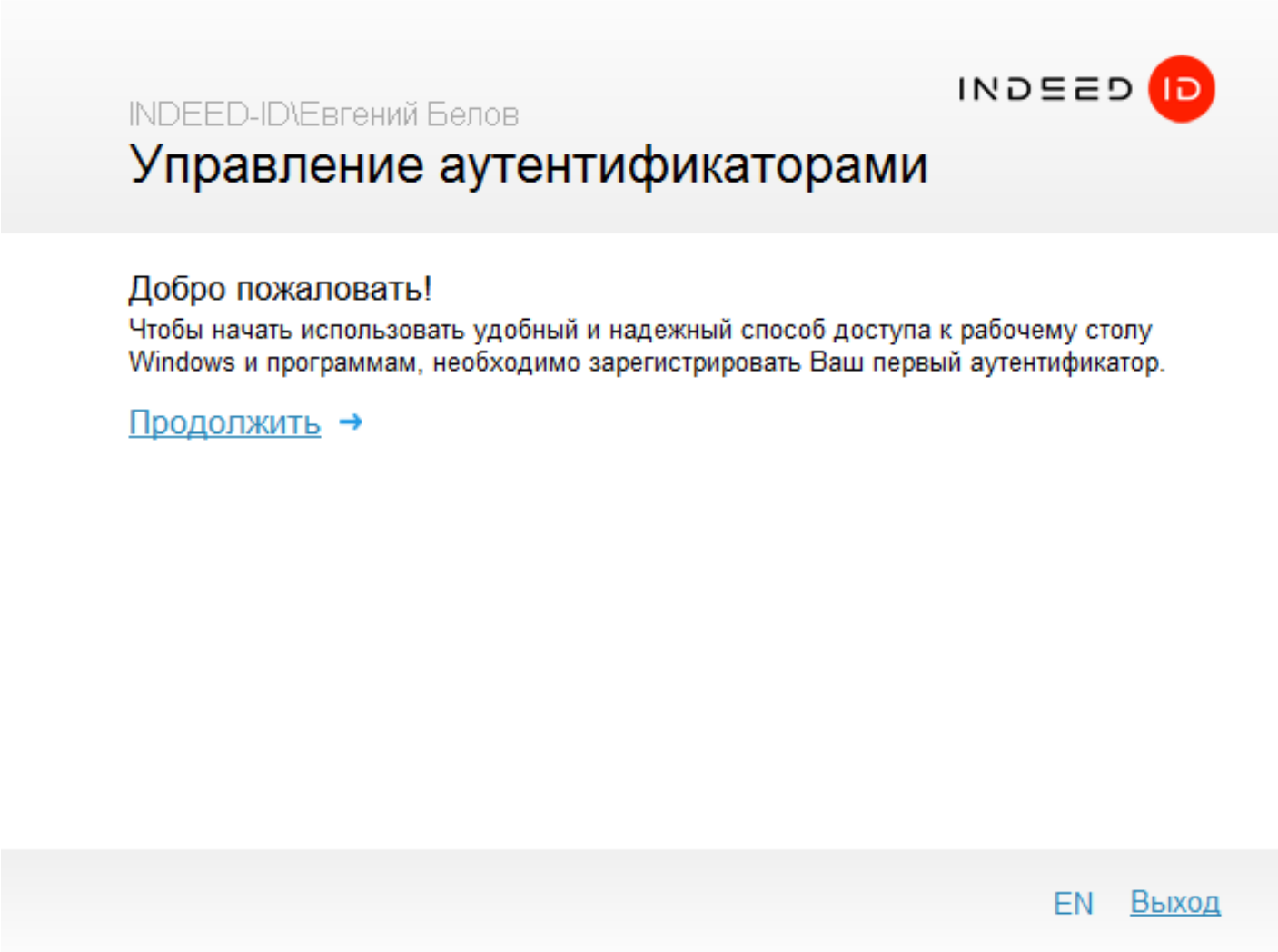

Рисунок 4 – Регистрация аутентификатора.

Если на рабочей станции пользователя установлено несколько провайдеров аутентификации, то необходимо выбрать **Одноразовый пароль (SMS OTP)** из списка (Рисунок 5). Если установлен только один провайдер, окно выбора не отображается. В случае использования провайдера Indeed-Id SMS OTP with PIN Provider выберите **Одноразовый пароль (SMS OTP + PIN)**.

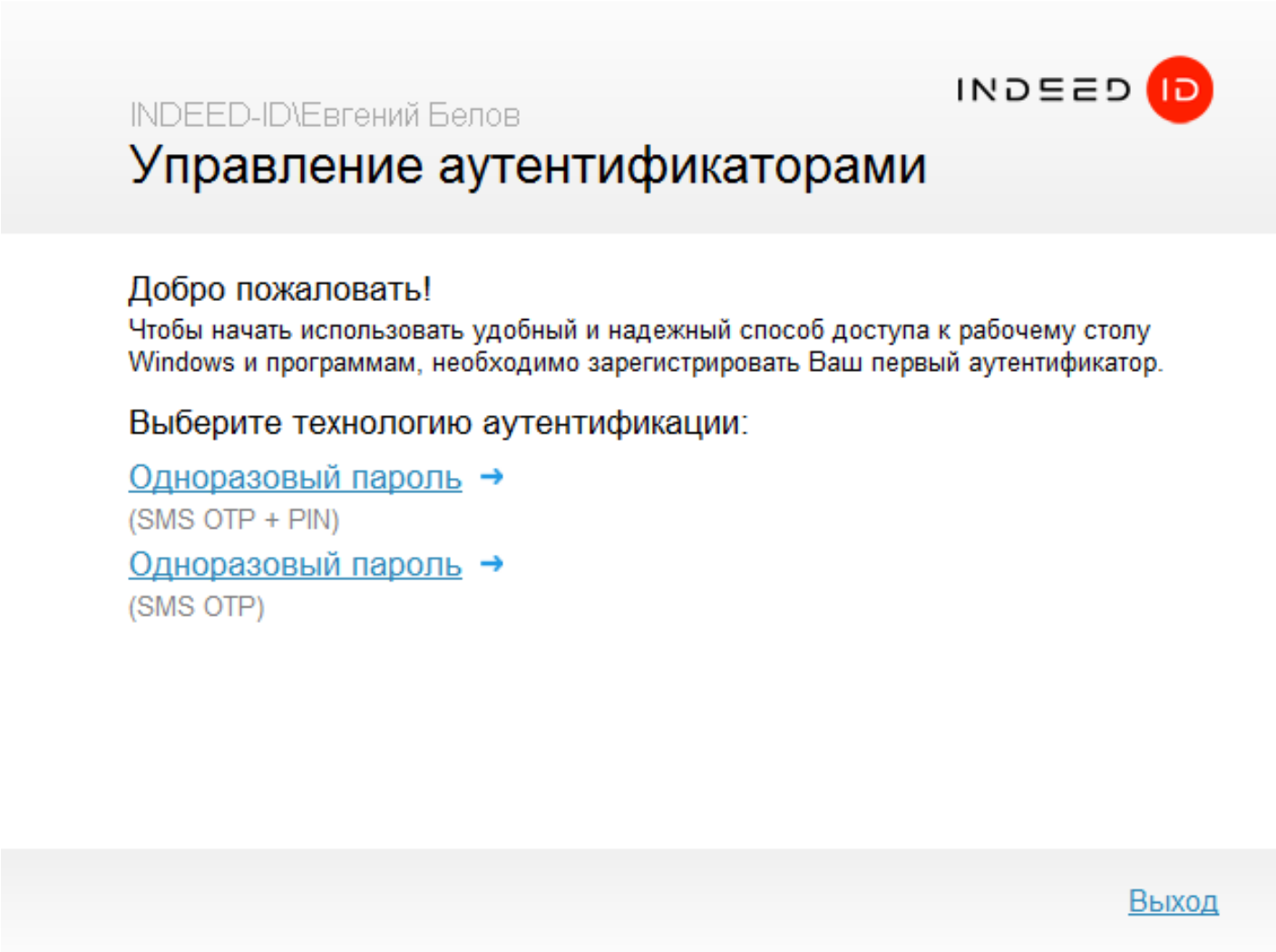

Рисунок 5 – Выбор аутентификатора.

Укажите номер мобильного телефона с кодом страны (код Российской Федерации – 7) и нажмите **Получить код** (Рисунок 6).

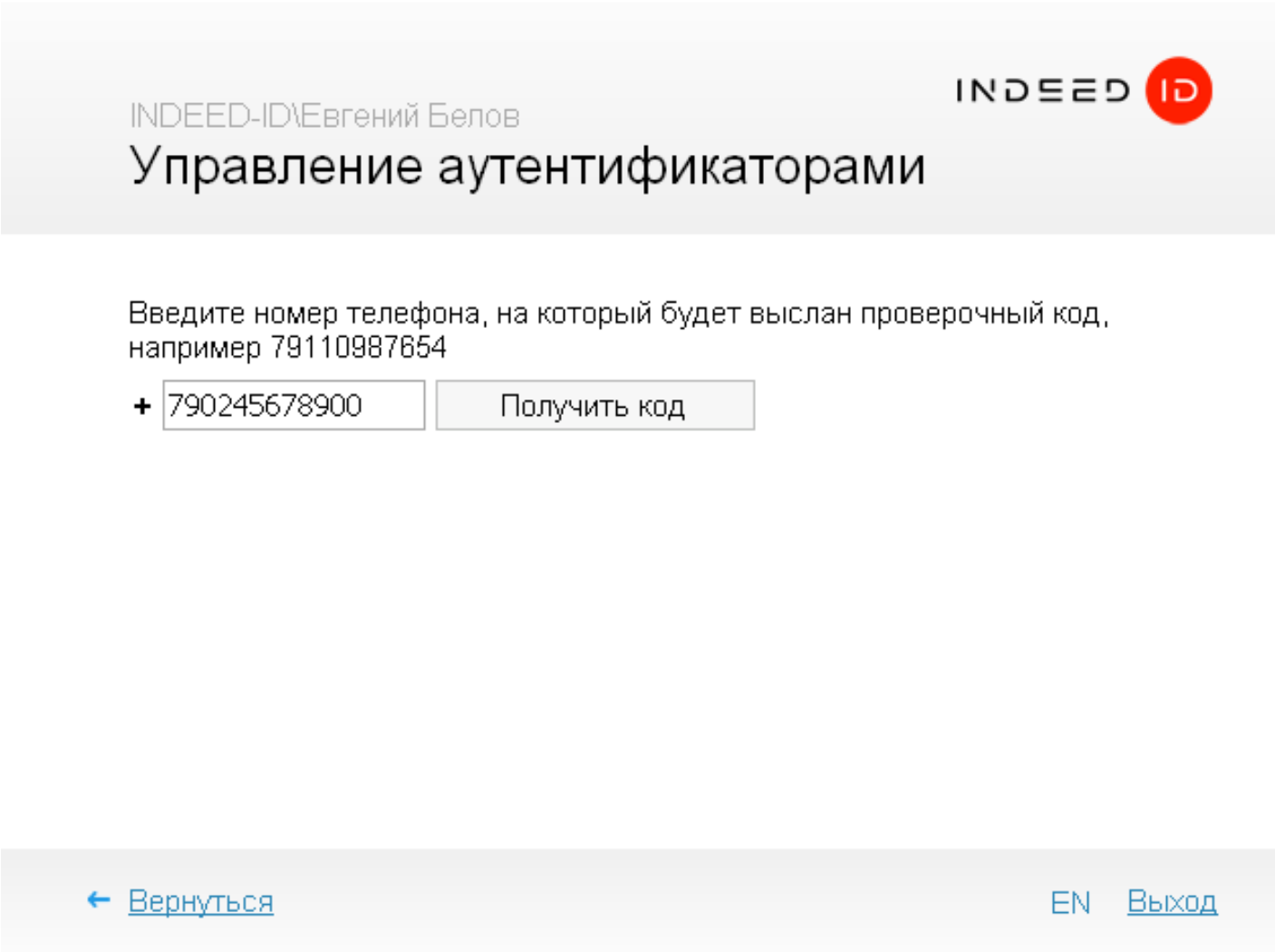

Рисунок 6 – Ввод номера телефона.

В случае использования провайдера Indeed-Id SMS OTP Provider with PIN потребуется придумать PIN-код и ввести его (Рисунок 7). Данный PIN-код необходимо будет вводить каждый раз при аутентификации пользователя дополнительно к одноразовому паролю из SMS.

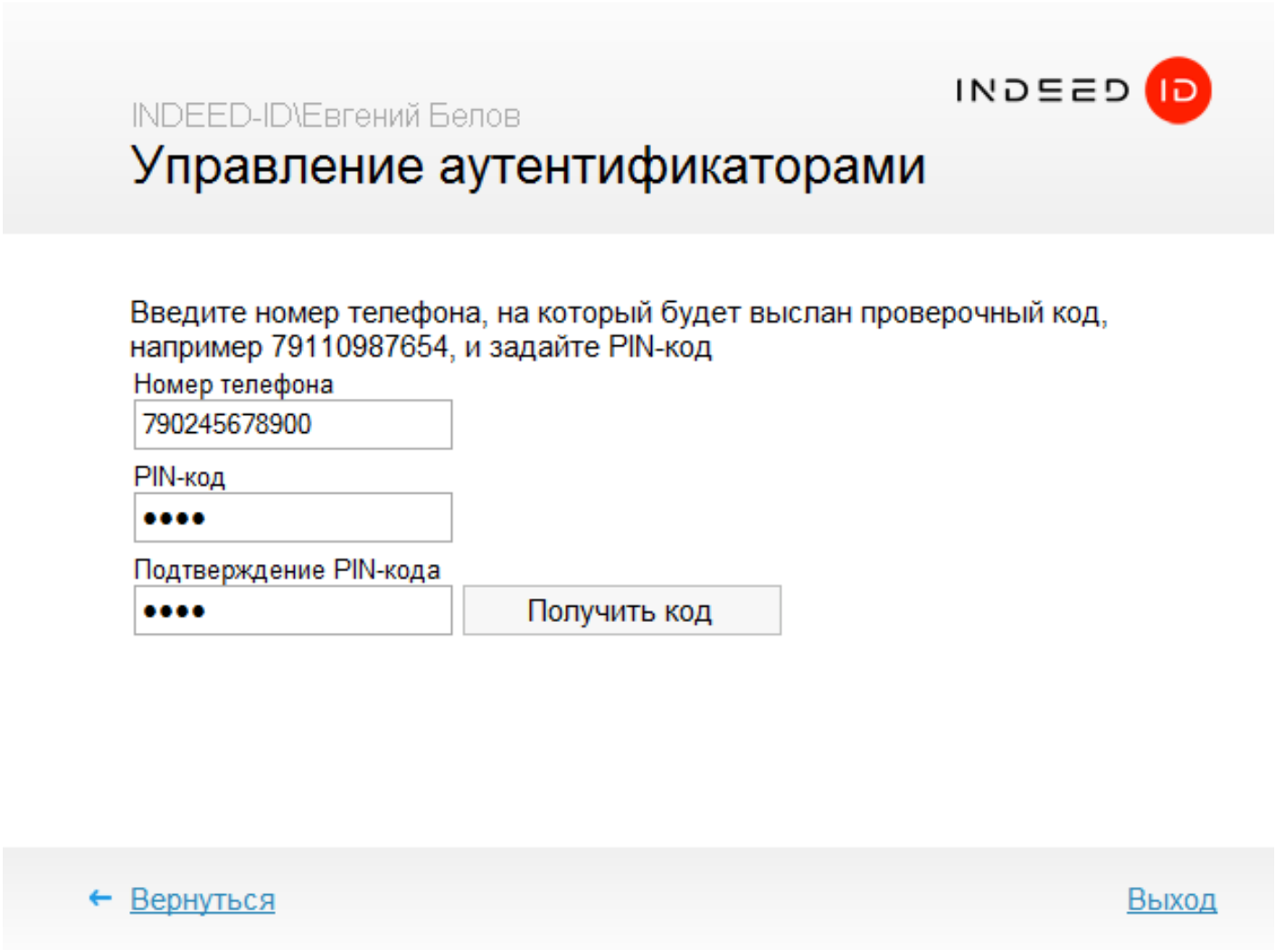

Рисунок 7 – Установка пользовательского PIN-кода.

На указанный номер придет сообщение с кодом. Например: **Ваш одноразовый пароль Indeed-Id: 34173c**. Введите полученный код и нажмите кнопку **Подтвердить** (Рисунок 8).

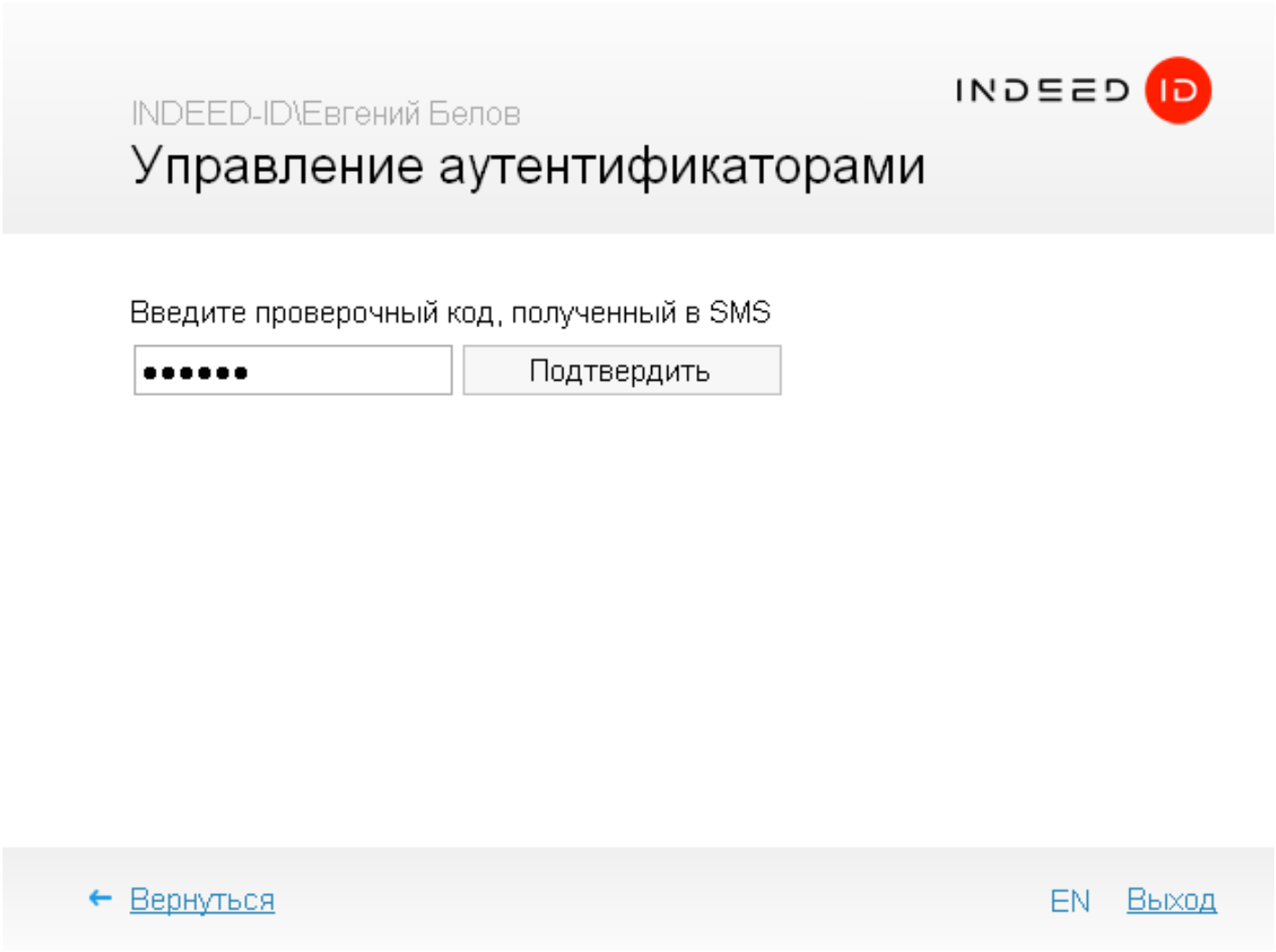

Рисунок 8 – Подтверждение полученного в SMS кода.

При необходимости, введите комментарий к заданному способу входа и нажмите **Сохранить** (Рисунок 9).

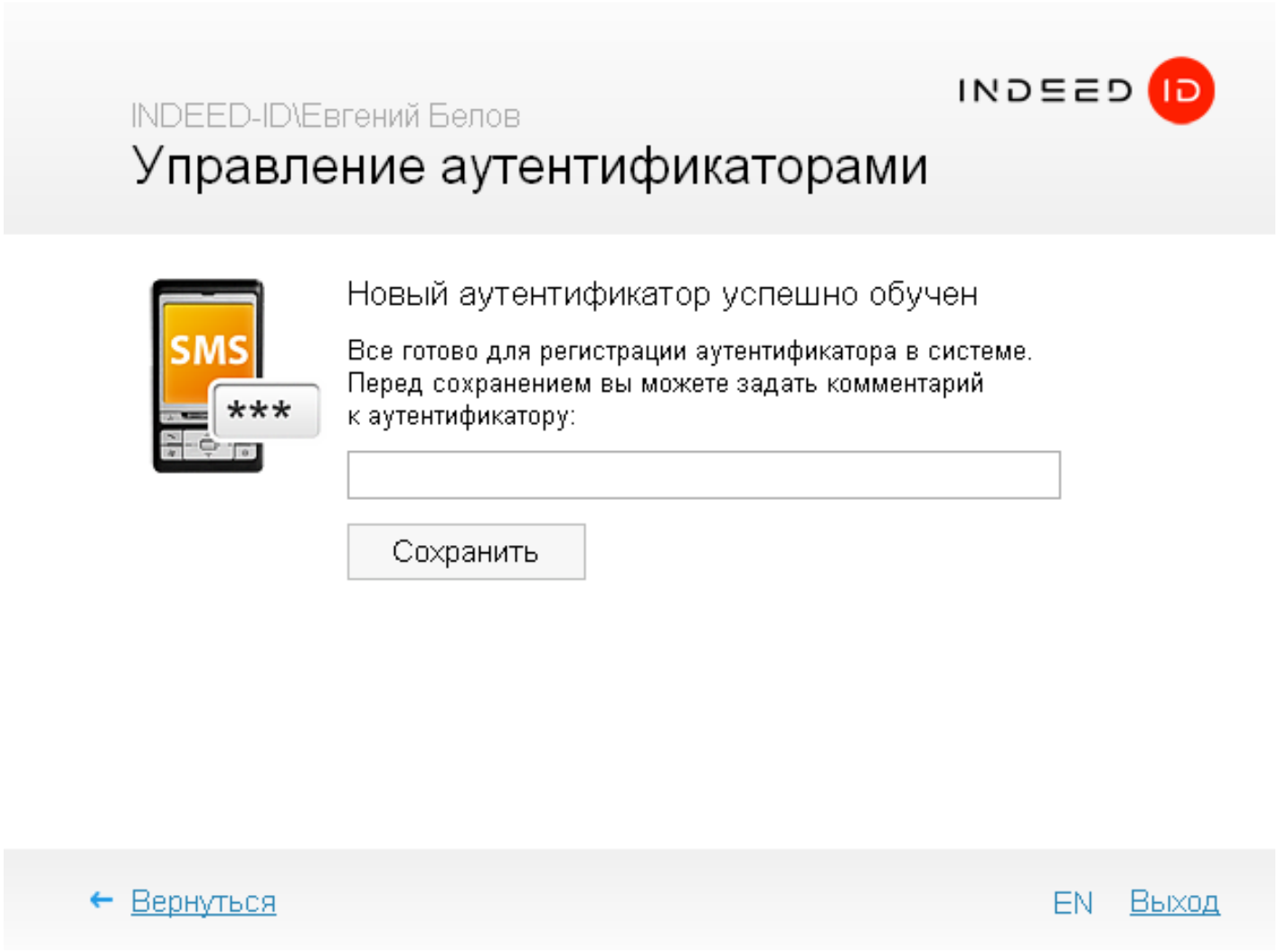

Рисунок 9 – Комментарий к аутентификатору.

После нажатия на кнопку **Сохранить** аутентификатор сохранится и его можно будет использовать для аутентификации. Нажмите **Выход** для завершения работы приложения **Indeed-Id Управление аутентификаторами**.

У одного пользователя системы Indeed Enterprise Authentication(Indeed Enterprise Single Sign-On) может быть одновременно зарегистрирован только один аутентификатор типа Indeed-Id SMS OTP, независимо от установленного администратором ограничения на максимальное количество аутентификаторов.

Аутентификация при помощи Indeed-Id SMS OTP Provider

При первом входе в систему или приложение с использованием технологии аутентификации Indeed-Id необходимо выбрать способ входа. Для этого нажмите **Сменить способ входа** (Рисунок 10) в окне **Вход в Windows** (окно **Аутентификация** для Enterprise SSO). Выберите способ входа **Одноразовый пароль (SMS OTP)** или **Одноразовый пароль (SMS OTP + PIN)**.

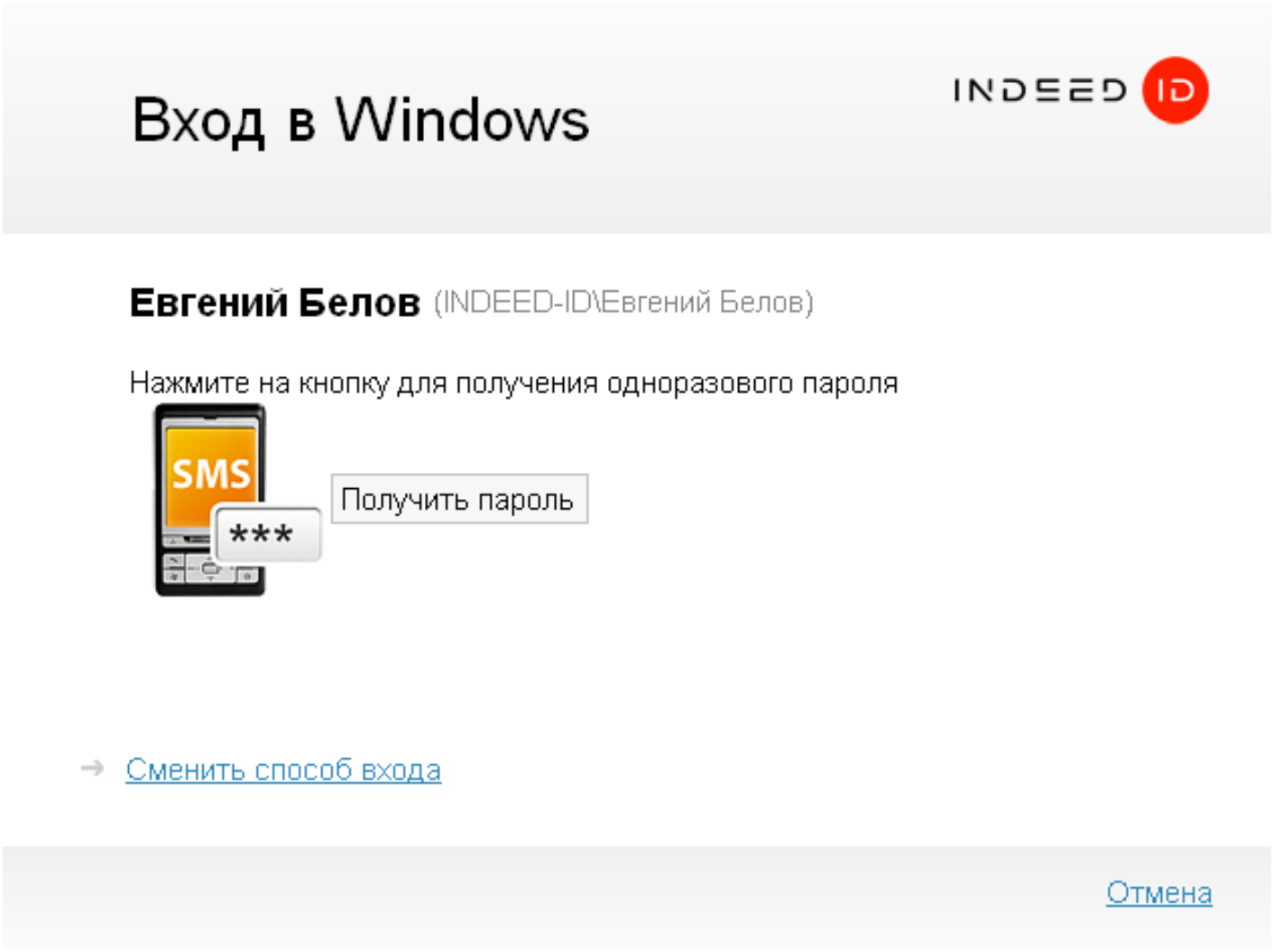

Рисунок 10 – Вход в Windows с помощью Indeed-Id SMS OTP.

В случае использования Indeed-Id SMS OTP Provider with PIN введите PIN-код, указанный при регистрации аутентификатора (Рисунок 11).

Рисунок 11 – Двухфакторная аутентификация по PIN-коду и одноразовому паролю.

Нажмите кнопку **Получить пароль**. На указанный номер придет сообщение с паролем. Например: **Ваш одноразовый пароль Indeed-Id: 1534b7**. Введите полученный пароль и нажмите кнопку **Вход** (Рисунок 12).

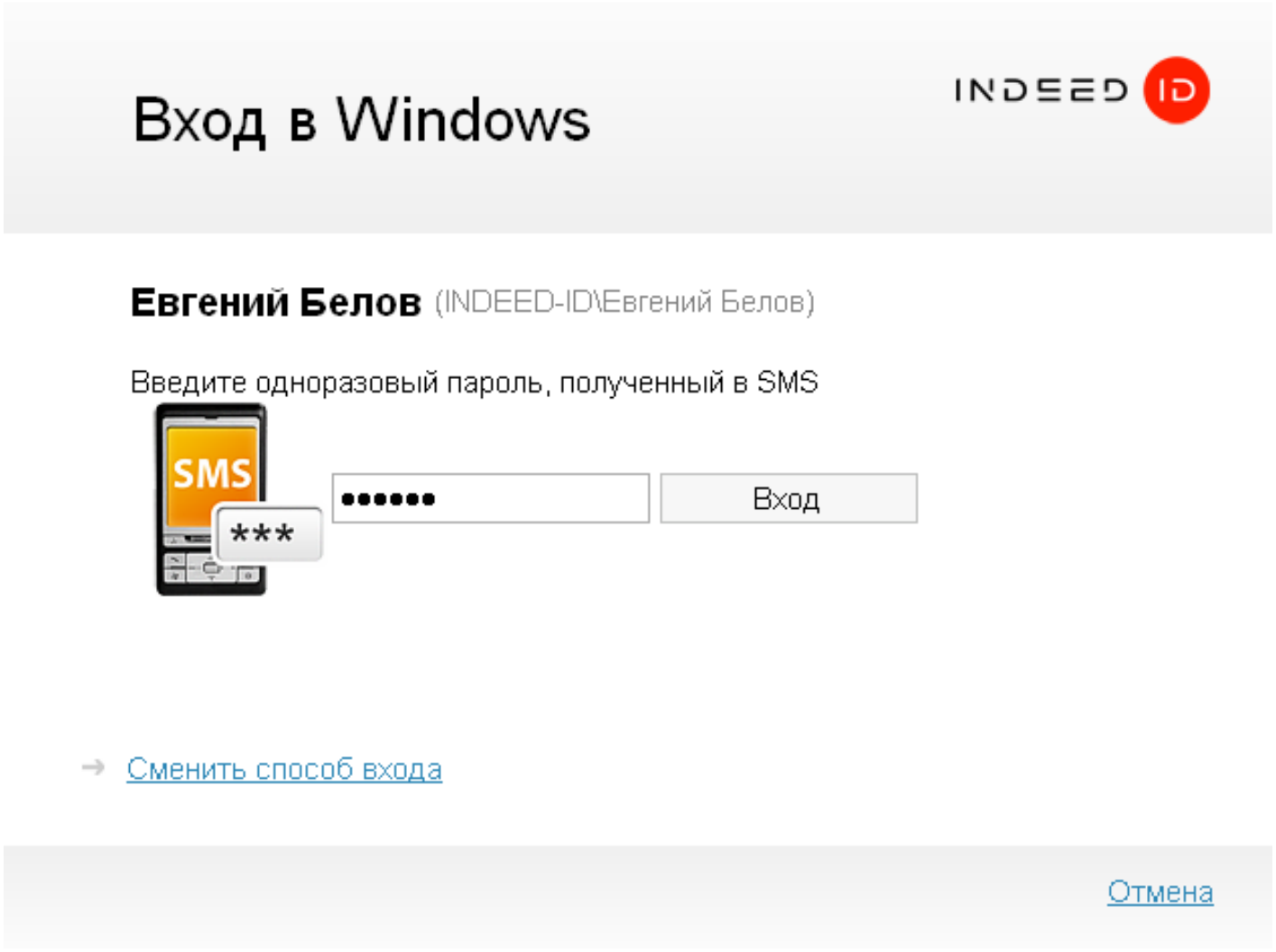

Рисунок 12 – Аутентификация при помощи Indeed-Id SMS OTP.

Если одноразовый пароль введен неверно, то появится сообщение об ошибке. Получите новый одноразовый пароль и повторите попытку аутентификации (Рисунок 13).

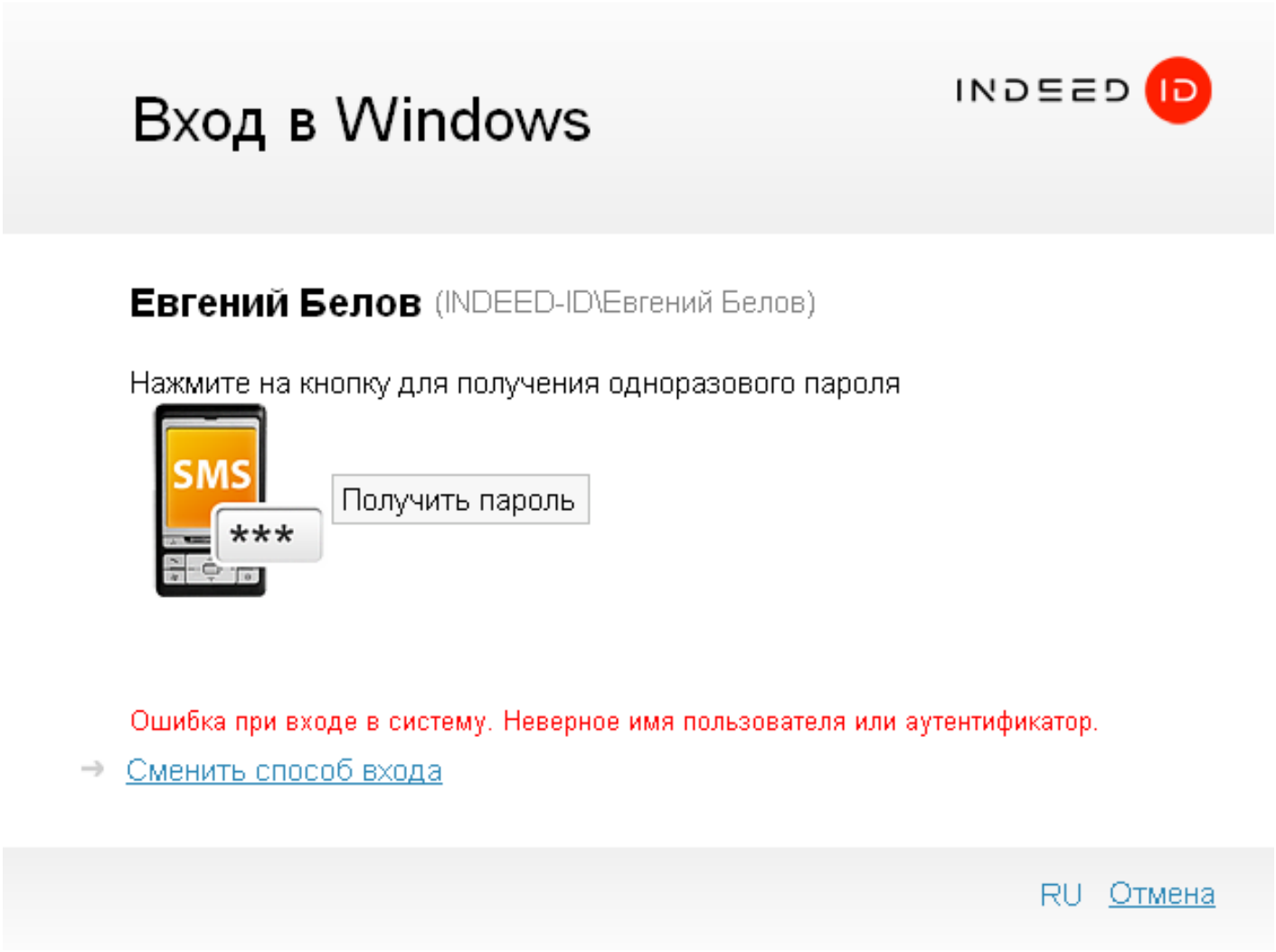

Рисунок 13 – Сообщение об ошибке при неверно введенном имени пользователя или аутентификаторе.

В случае успешного входа по аутентификатору, способ входа **Одноразовый пароль (SMS OTP)** или **Одноразовый пароль (SMS OTP + PIN)** запоминается как предпочтительный и будет автоматически предложен пользователю при следующем входе в систему или приложение.

Использование Indeed-Id SMS OTP Provider с Indeed NPS RADIUS Extension

Indeed-Id SMS OTP Provider может быть использован для аутентификации пользователей в RADIUS-сервисах[4]. В этом случае в процессе аутентификации пользователя сервер Indeed EA сформирует одноразовый пароль и отправит его на сервер SMPP, а тот в свою очередь отправит его на номер, указанный в профиле пользователя Active Directory.

Если номер телефона не задан или указан неверно, то пароль не будет отправлен, а на сервере Indeed EA будет зафиксировано соответствующее событие.

Для использования Indeed-Id SMS OTP Provider совместно с Indeed NPS RADIUS Extension никаких действий по установке и регистрации провайдера со стороны пользователя не требуется. Провайдер устанавливается только на серверах Indeed EA (ESSO).

На Рисунке 14 приведен пример аутентификации пользователя в интерфейсе приложения Citrix NetScaler с использованием Indeed-Id SMS OTP Provider.

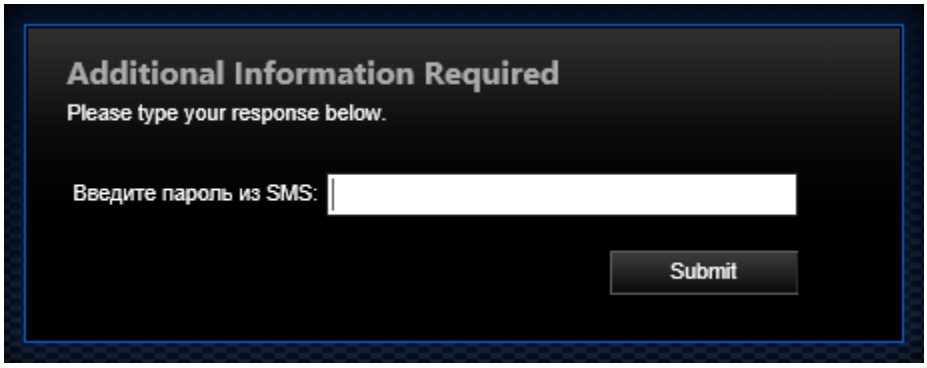

Рисунок 14 – Аутентификация в Citrix NetScaler с использованием Indeed-Id SMS OTP Provider.

[4]Только версия без PIN-кода.

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*.

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.

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).

Подробнее об управлении аутентификаторами смотрите в документах *Indeed-Id Enterprise SSO. Руководство пользователя.pdf* и *Indeed-Id Windows Logon. Руководство по установке и использованию.pdf*.