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 OTM Provider

Руководство по установке и эксплуатации

версия 1.5.1

Содержание

Введение

Приветствуем вас и благодарим за приобретение программных продуктов компании Indeed ID. Это руководство поможет вам ознакомиться с принципом работы компонента **Indeed-Id OTM 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 OTM Provider

Компонент Indeed-Id OTM Provider предназначен для аутентификации пользователей с применением технологии одноразовых паролей и совместного использования с продуктами Indeed Enterprise Authentication и Indeed Enterprise Single Sign-On. Генерация случайных паролей происходит по технологии One Time Matrix (OTM). В основе технологии доступа OTM лежит использование одноразового пароля, который формируется путем распознавания заданного шаблона и последовательного считывания цифр, отображенных в ячейках шаблона.
Под шаблоном понимается последовательность ячеек одноразовой матрицы, выбранная пользователем, сохраненная в системе и используемая в качестве эталонного аутентификатора. Набор цифр в ячейках матрицы генерируется случайным образом при каждой попытке аутентификации, что исключает возможность повторного использования одного и того же кода доступа (см. Рисунок 1, Рисунок 2 и Рисунок 3). Цифра в ячейке на Рисунке 2 указывает, какой по счету была выбрана ячейка пользователем.
Одноразовый пароль, соответствующий заданному на Рисунке 2 шаблону – **349051**. Технология доступа OTM проста и удобна, поскольку основана на зрительной памяти и не требует запоминания цифр и символов. Преимуществами OTM также являются экономичность (не требуется приобретение и установка дополнительного оборудования) и гибкость (возможна настройка сложности шаблонов и установка ограничений в зависимости от требуемого уровня безопасности).

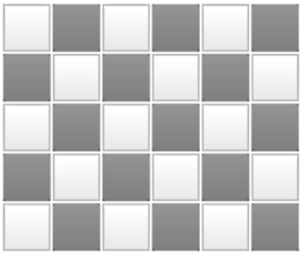

Рисунок 1 – Пустой шаблон матрицы.

Рисунок 2 – Заданный шаблон матрицы.

Рисунок 3 – Заполненная матрица.

Работа с Indeed-Id OTM Provider

Регистрация аутентификатора

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

Аутентификатор регистрируется после установки на рабочую станцию пользователя компонентов Indeed EA(ESSO): Indeed-Id Windows Logon или Indeed-Id ESSO Агент (в зависимости от используемой конфигурации) и провайдера Indeed-Id OTM Provider. Пользователь выполняет вход в мастер регистрации аутентификатора по доменному паролю и, следуя указаниям приложения **Indeed-Id Управление аутентификаторами**, регистрирует аутентификатор.

Для регистрации аутентификатора пользователю, от имени которого осуществляется регистрация, должно быть 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 операционную систему, регистрацию можно выполнить в любой удобный момент, запустив приложение **Indeed-Id Управление аутентификаторами** из меню *Пуск – Все программы – Indeed-Id*.

Для регистрации аутентификатора выполните вход в мастер первого входа (утилиту Indeed-Id Управление аутентификаторами) по доменному паролю и выполните следующие действия: В окне **Управление аутентификаторами** нажмите **Продолжить** (Рисунок 4).

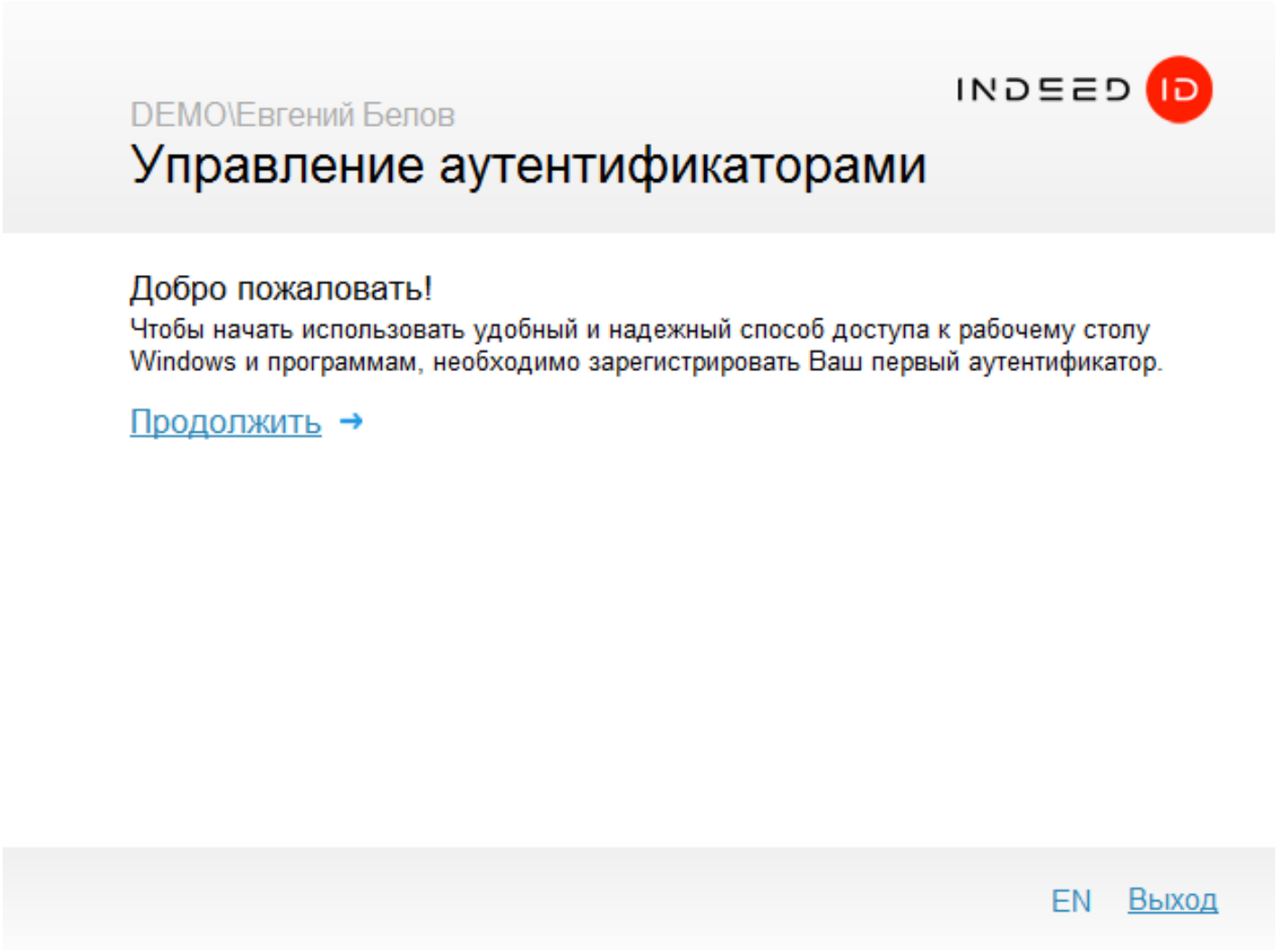

Рисунок 4 – Регистрация аутентификатора.

Если на рабочей станции пользователя установлено несколько провайдеров аутентификации, то необходимо выбрать **Одноразовая матрица (Indeed-Id OTM)** из списка (Рисунок 5). Если установлен только один провайдер, окно выбора не отображается.

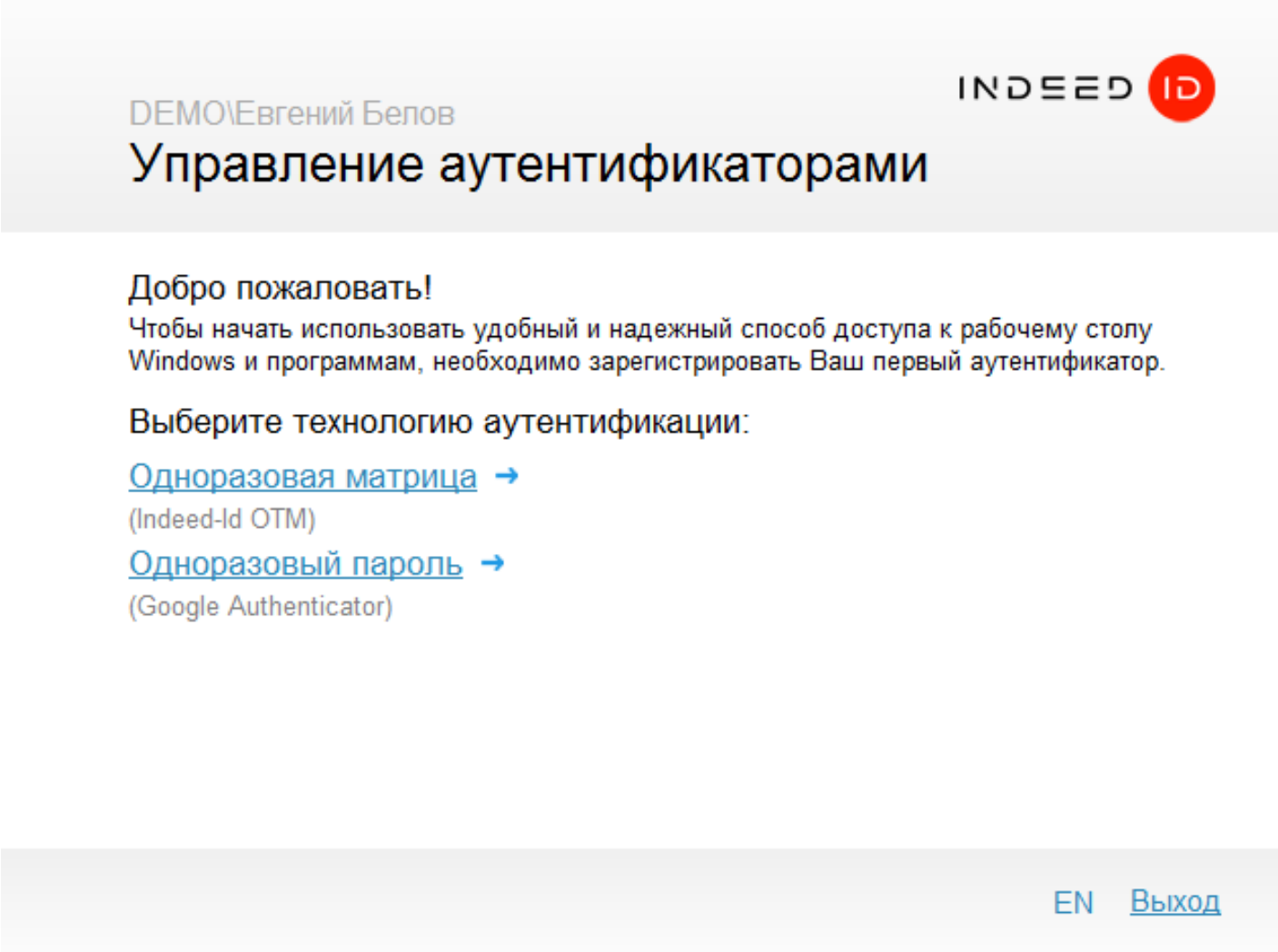

Рисунок 5 – Выбор аутентификатора.

Нажимая на ячейки таблицы, задайте шаблон (Рисунок 6).

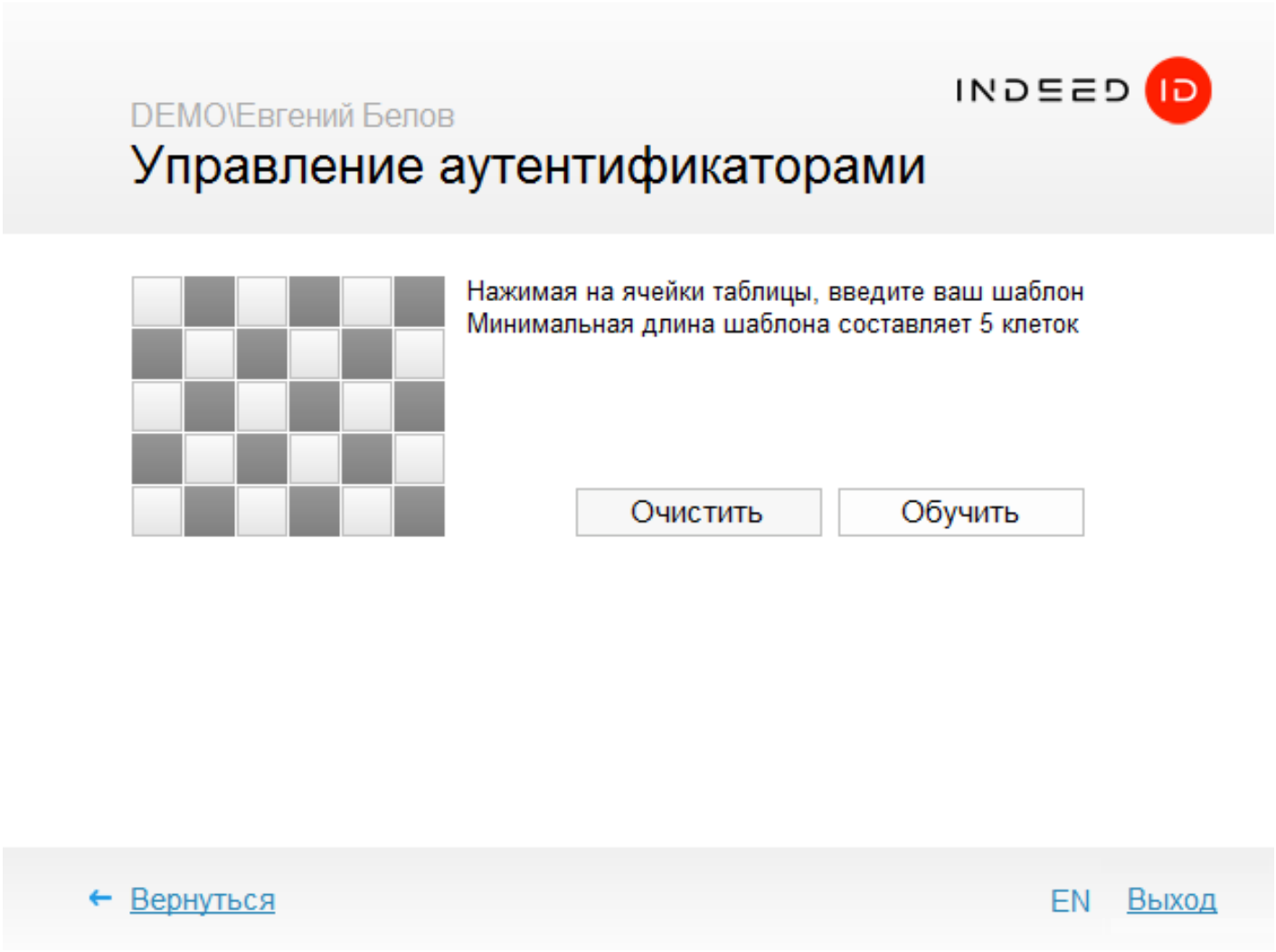

Рисунок 6 – Пустое поле матрицы.

Минимальная длина шаблона по умолчанию составляет 5 клеток (Рисунок 7).

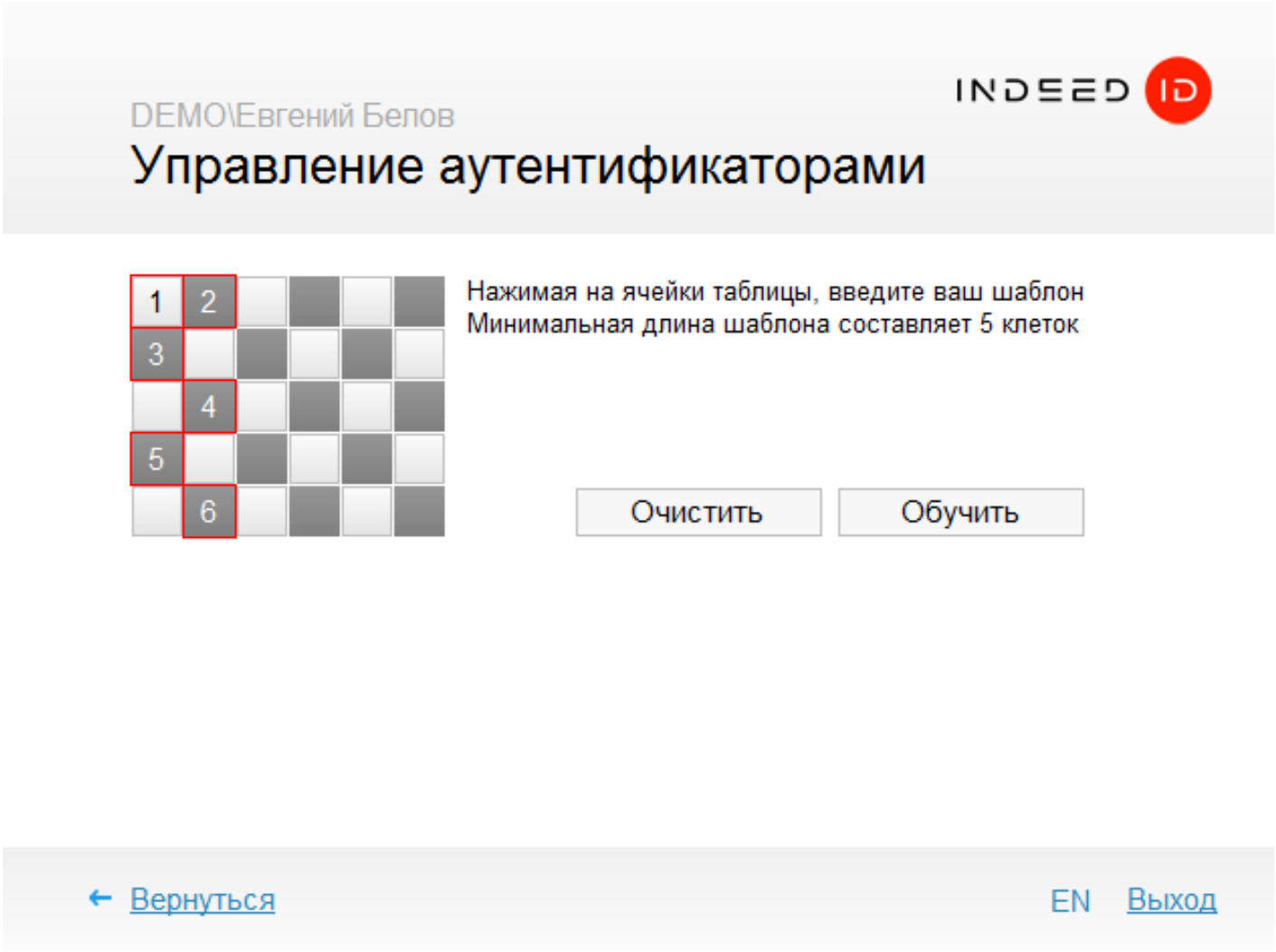

Рисунок 7 – Заданный пользователем шаблон.

Шаблон не должен содержать более 3-х (значение по умолчанию) клеток подряд из одной диагонали. Нажмите **Обучить** для сохранения шаблона или **Очистить** для создания нового шаблона. Параметры, определенные по умолчанию могут быть изменены (см. **Настройка параметров аутентификации** на стр. 13).

При необходимости, введите комментарий к заданному способу входа и нажмите **Сохранить** (Рисунок 8).

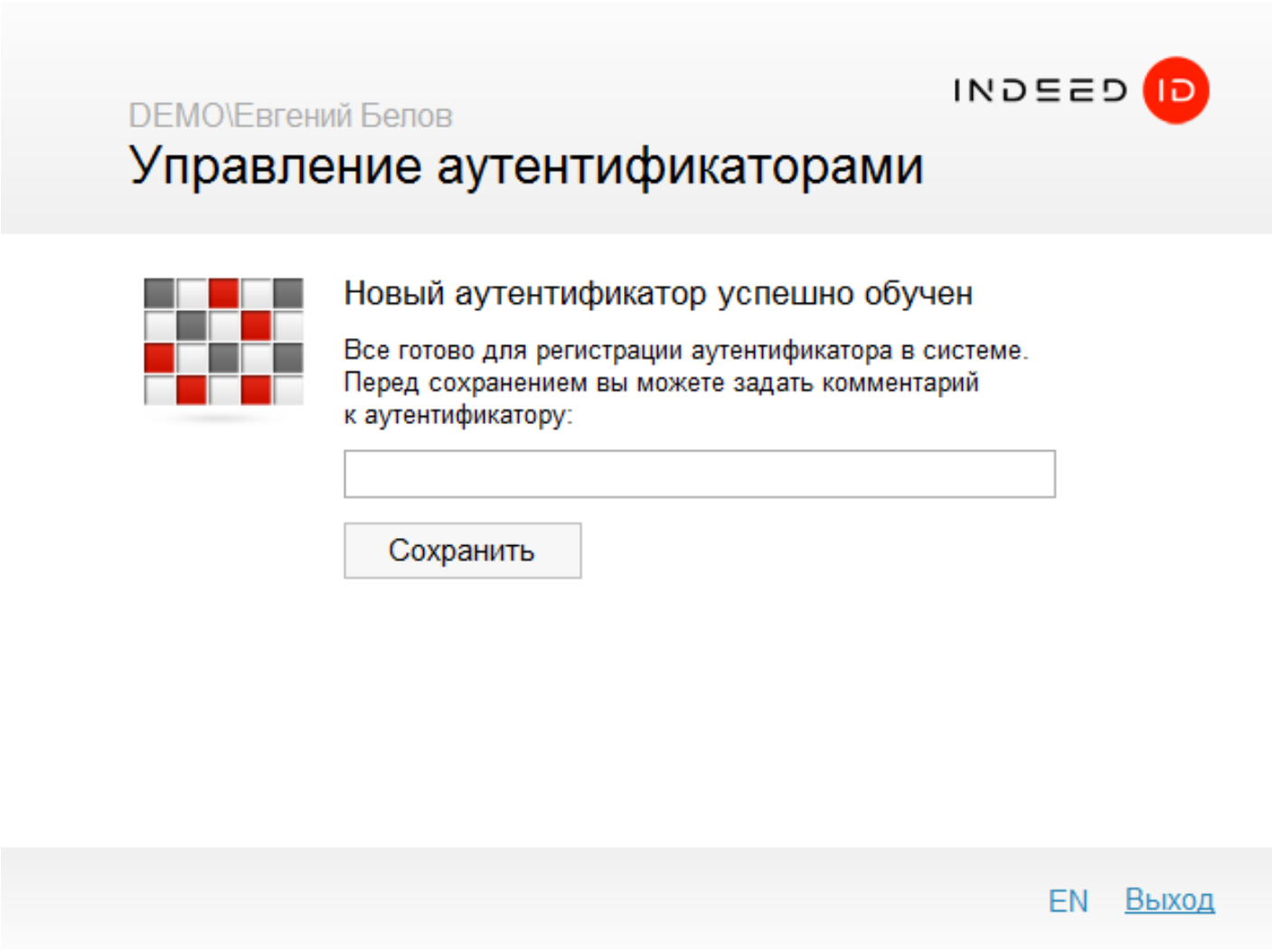

Рисунок 8 – Комментарий к аутентификатору.

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

Аутентификация при помощи Indeed-Id OTM Provider

При первом входе в операционную систему или приложение с использованием технологии аутентификации Indeed-Id выберите способ входа. Для этого нажмите **Сменить способ входа** (Рисунок 9) в окне **Вход в Windows** (окно **Аутентификация** для Enterprise SSO). Выберите способ входа **Одноразовая матрица**.

Рисунок 9 – Вход в Windows с помощью Indeed-Id OTM.

Вспомните форму шаблона и введите цифры в той последовательности, в которой были выбраны ячейки шаблона при регистрации аутентификатора и нажмите **Вход**. Если одноразовый пароль введен неверно, то появится сообщение об ошибке, а матрица автоматически обновится и заполнится новыми цифрами (Рисунок 10).

Рисунок 10 – Сообщение об ошибке при неверно введенном имени пользователя или аутентификаторе.

В случае успешного входа по аутентификатору, способ входа **Одноразовая матрица** запоминается как предпочтительный и будет автоматически предложен пользователю при следующем входе в операционную систему или приложение.

Управление аутентификаторами

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

- обучать
- переобучать
- 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*.

Установка Indeed-Id OTM Provider

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

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

Для развертывания Indeed-Id OTM 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 OTM Provider выполните следующие действия:

1. Запустите файл IndeedID.OTM.Provider.msi 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.

Настройка параметров аутентификации

В этом разделе содержится описание настраиваемых параметров работы Indeed-Id OTM Provider и способах их изменения. Изменение параметров работы Indeed-Id OTM Provider осуществляется через механизм групповых политик Active Directory.

Настройка политик необходима для повышения уровня безопасности. Однако полноценная работа Indeed-Id OTM Provider возможна и со значениями политик, определенными по умолчанию.

Перед настройкой групповой политики необходимо добавить в список административных шаблонов шаблоны политик Indeed-Id. Административный файл шаблона политики входит в состав дистрибутива и расположен в каталоге Misc.

Для получения подробной информации обратитесь к документу *Indeed-Id Admin Pack. Руководство по установке и использованию.pdf*.

Группа политик **One time matrix provider** определяет следующие параметры использования технологии аутентификации One Time Matrix (OTM):

- Минимальная длина шаблона
- Ширина матрицы
- Настройка сложности шаблона

Минимальная длина шаблона Политика определяет минимальное количество ячеек в шаблоне пользователя. Значение по умолчанию: 5 ячеек.

Ширина матрицы Политика определяет ширину матрицы. Значение по умолчанию: 6 ячеек.

Настройка сложности шаблона Политика определяет параметры, которые будут учитываться при создании шаблона пользователем. Если политика отключена, пользователь не имеет ограничений при создании шаблона. С помощью политики можно установить следующие параметры:

- Запрещено использовать 4 угловые клетки в шаблоне
- Запрещено использовать строку в качестве шаблона
- Запрещено использовать столбец в качестве шаблона
- Запрещено использовать N клеток подряд на одной диагонали в шаблоне (если политика включена, значение данной настройки по умолчанию равно 3).

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