Выполнение требований стандарта PCI DSS в части аутентификации пользователей

В апреле 2016 года была принята новая версия **PCI DSS 3.2.** Часть нововведений этой версии вступает в силу 1 февраля 2018 года. К таким нововведениям относятся изменения в части аутентификации сотрудников при доступе к информационным системам банка. Так, с 01.02.2018 г. становится обязательным применение многофакторной аутентификации в ряде сценариев доступа.

Indeed Access Manager (**Indeed AM**) является универсальной системой аутентификации, предназначенной для организации строгой и мультифакторной аутентификации в любых системах, используемых на предприятиях: ОС, web- и мобильные приложения, VPN, VDI, SAML-совместимые приложения и др. Поддерживается также технология **Enterprise Single Sign-On**.

Ниже приведены комментарии по реализации конкретных требований стандарта **PCI DSS 3.2** в части аутентификации с использованием программного обеспечения **Indeed Identity**.

Требование PCI DSS 3.2	**Перевод требования**	**Комментарий**
8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts. 8.1.6.a For a sample of system components, inspect system configuration settings to verify that authentication parameters are set to require that user accounts be locked out after not more than six invalid logon attempts.	8.1.6 Блокировать учетные записи после шести неудачных попыток входа подряд. 8.1.6.a Сделать выборку системных компонентов, проверить настройки системной конфигурации и убедиться в том, что учетная запись пользователя блокируется после не более чем шести неудачных попыток входа.	**Indeed Access Manager** позволяет централизованно задавать политику блокировки способов входа при превышении заданного числа попыток аутентификации.
8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: • Something you know, such as a password or passphrase • Something you have, such as a token device or smart card • Something you are, such as a biometric.	8.2 Помимо назначения уникального идентификатора, для обеспечения надлежащего управления аутентификацией сотрудников (не пользователей) и администраторов на уровне всех системных компонентов должен применяться хотя бы один из следующих методов аутентификации всех пользователей: • то, что вы знаете (например, пароль или парольная фраза); • то, что у вас есть (например, ключи или смарт-карты); • то, чем вы обладаете (например, биометрические параметры).	Применение продуктов **Indeed Certificate Manager** и **Indeed Access Manager** позволяет использовать все указанные методы аутентификации. При этом, в зависимости от окружения, сотруднику могут быть доступны различные варианты аутентификации (например, смарт-карта + PIN-код при доступе в ОС и пароль + OTP при доступе в VPN).

8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication	8.3 Защита не консольного административного доступа и удаленного доступа для всех пользователей к информационной среде держателей карт с помощью мультифакторной аутентификации.	Требование может быть выполнено как с использованием PKI (public key infrastructure), так и без него. Также возможно совмещение технологий, например, таким образом: • Применение смарт-карт и цифровых сертификатов для аутентификации в локальном режиме работы (в ОС и приложениях); • Применение технологии одноразовых паролей для удаленного доступа (например, при аутентификации в VPN). Выбор конкретных технологий будет зависеть от используемого программно-аппаратного обеспечения. Кроме того, выбор технологии может зависеть от полномочий и роли пользователя (например, сертификаты для сотрудников и SMS для третьих лиц). **ПО Indeed CM** и **Indeed AM** позволяет реализовать на практике любой сценарий аутентификации, без привязки к конкретным технологиям.
8.3.1 Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.	8.3.1 Применение мультифакторной аутентификации для не консольного доступа к информационной среде держателей карт для сотрудников с административным доступом.	
8.3.2 Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside the entity's network.	8.3.2 Применение мультифакторной аутентификации для средств удаленного доступа сотрудников (включая пользователей и администраторов) и любых третьих лиц (включая доступ поставщиков для поддержки или техобслуживания) во внутреннюю сеть из внешней сети.	