Microsoft Forefront Identity Manager FIM

Microsoft Forefront Identity Manager (FIM) – система автоматизации управления идентификационной информацией сотрудников: учетными записями и правами доступа пользователей к информационным ресурсам компании.

Преимущества в области информационной безопасности:

права доступа каждого сотрудника определяются и контролируются автоматически в соответствии с требуемой бизнес-логикой;

все изменения полномочий сотрудников автоматически отслеживаются и фиксируются.

Внедрение системы FIM (+Indeed-ID) позволит организации выполнить ряд ключевых требований Федерального Законодательства и отраслевых стандартов в области ИБ. В частности выполняются требования:

- Федерального Закона №152-ФЗ «О персональных данных»;
- Федерального Закона №161-ФЗ «О национальной платежной системе»;
- Стандарт Банка России по ИБ (СТО БР ИББС-1.0-2010);
- Стандарта безопасности данных индустрии платежных карт (PCI DSS v 2.0).

Целевая аудитория

1.Кредитно-финансовые учреждения, страховые компании, лизинговые компании

2.Любые компании, которые:

- имеют множество подразделений;
- имеют численность персонала более 500 человек, работающих в информационных системах;
- работают в условиях интенсивной смены персонала в отдельных подразделениях;
- имеют богатый и/или гетерогенный IT-ландшафт (различные источники данных, бизнес-системы);
- пользуются услугами аутсорсинга;
- не имеют инструментов для отслеживания изменений прав доступа, где существуют значительные риски несанкционированного доступа к важной корпоративной информации.

Эффективность

Сокращение времени предоставления новому сотруднику прав доступа в информационные системы в соответствии с ролевой моделью.

Повышение информационной безопасности благодаря мониторингу кадров – оперативное получение информации об изменениях ролевых моделей сотрудников, о перемещениях персонала, об увольнениях.

Упрощение процессов управления идентификацией и доступом пользователей благодаря порталу самообслуживания пользователей и целому набору инструментов для администраторов.

Автоматизация типовых задач управления учетными записями, паролями, группами и списками рассылки, а также цифровыми сертификатами пользователей.

Возможность самостоятельной подачи запросов на изменение прав доступа и операции с персональными данными.

Функциональные возможности

- Центр управления идентификационными данными пользователей
- Единый инструмент контроля и аудита полномочий сотрудников в информационных системах
- Модели и репозитории прав доступа сотрудников
- Модуль обеспечения основных функций решений класса ServiceDesk
- Платформа для обеспечения процессов согласования и обработки пользовательских заявок (в т. ч. прав доступа сотрудников)
- Хранилище данных о нештатных сотрудниках компании

Система управления идентификационными данными Indeed-Id

Система управления идентификационными данными Indeed-Id – это система класса Identity and Access Management (IAM), обеспечивающая централизованное управление учетными данными сотрудников и их доступом к информационным ресурсам компании.

Целевая аудитория

Любое предприятие, заинтересованное в защите своих информационных ресурсов

Эффективность

- Доступ сотрудников к рабочему столу через выбранную процедуру аутентификации:

Контактные смарт-карты и USB-ключи

Бесконтактные карты

> 20 способов аутентификации

Биометрия

Одноразовый пароль с использованием различных способов доставки

Это исключает необходимость запоминать логины и пароли, решаются проблемы утраты пароля или передачи его другим лицам.

- Доступ к большинству корпоративных ресурсов через Indeed-Id с помощью универсальной процедуры аутентификации (Single Sign-On).
- IT-администраторы используют гибкие инструменты регулирования условий доступа, что значительно сокращает объемы работы по его предоставлению или изменению.
- Следование регламентам ИБ, увеличивает эффективность предотвращения и оперативного расследования инцидентов.

Преимущества использования Indeed-ID

Сотрудники:

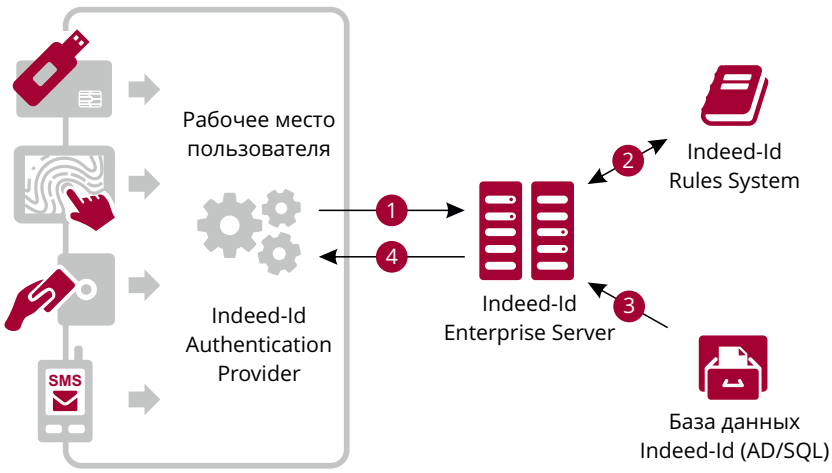
- Единая универсальная точка доступа к корпоративным информационным ресурсам

Служба ИТ:

- Удобный инструмент для управления доступами к ресурсам ИТ;
- Снижение количества обращений типа «Забыт пароль».

Служба ИБ:

- Выполнение требований информационной безопасности; Инструмент для проведения аудита доступа к ресурсам ИТ.



1. Получение аутентификатора от пользователя
2. Проверка разрешения на аутентификацию
3. Проверка аутентификатора на сервере
4. Ответ сервера.