



Банк высокой культуры

Что нужно знать, чтобы внедрить IDM? Место IDM в системе ИБ предприятия

Скородумов Анатолий Валентинович

Заместитель директора –

Начальник Управления по обеспечению информационной безопасности

Цели внедрения системы IDM

- Сокращение времени предоставления сотруднику необходимых прав доступа
- Снижение нагрузки на администраторов АС
- Повышение уровня информационной безопасности
- Повышение прозрачности управления доступом
- Упрощение процедур оформления и согласования прав доступа



Определение источников данных и целевых систем

Основной источник – АС учета кадров

Необходимо также определиться с источником для загрузки внештатных сотрудников



Целевые системы – все системы, с которыми работает большинство сотрудников организации, а также системы, скорость предоставления доступа к которым критична для бизнеса

Необходимо определиться с порядком предоставления доступа к остальным АС.

Функциональные требования

- Интеграция с системами управления кадрами
- Учет и хранение данных о правах пользователей в АС
- Наличие готовых коннекторов к эксплуатируемым АС
- Управление жизненным циклом учетных записей
- Реализация основных процедур, связанных с персоналом: прием на работу, увольнение, перемещение и т.д.
- Наличие портала самообслуживания
- Гибкая реализация логики согласования прав доступа
- Развитая отчетность, наличие построителя отчетов
- Контроль отсутствия в системах незарегистрированных в IDM учетных записей

Критерии выбора IDM

- Соответствие сформированным функционально-техническим требованиям
- Политика лицензирования и стоимость лицензий
- Стоимость внедрения и владения
- Наличие готовых коннекторов к эксплуатируемым АС
- Наличие успешных внедрений (прежде всего в России)
- Наличие русскоязычного интерфейса и тех поддержки
- Оценка рейтинговых агентств
- Заявленные сроки внедрения
- Требования к аппаратной платформе
- Удобство использования

Зрелость процессов ИБ и ИТ

- Наличие ролевых моделей
- Наличие формализованных процедур согласования прав доступа
- Наличие перечня информационных активов (ресурсов)
- Реализация ИТ-процессов по управлению инцидентами и управлению изменениями

ВАЖНО!!!!!!!!!!!!!!!!!!!!!!

IDM необходимо внедрять, когда организация находится в относительно стабильном состоянии

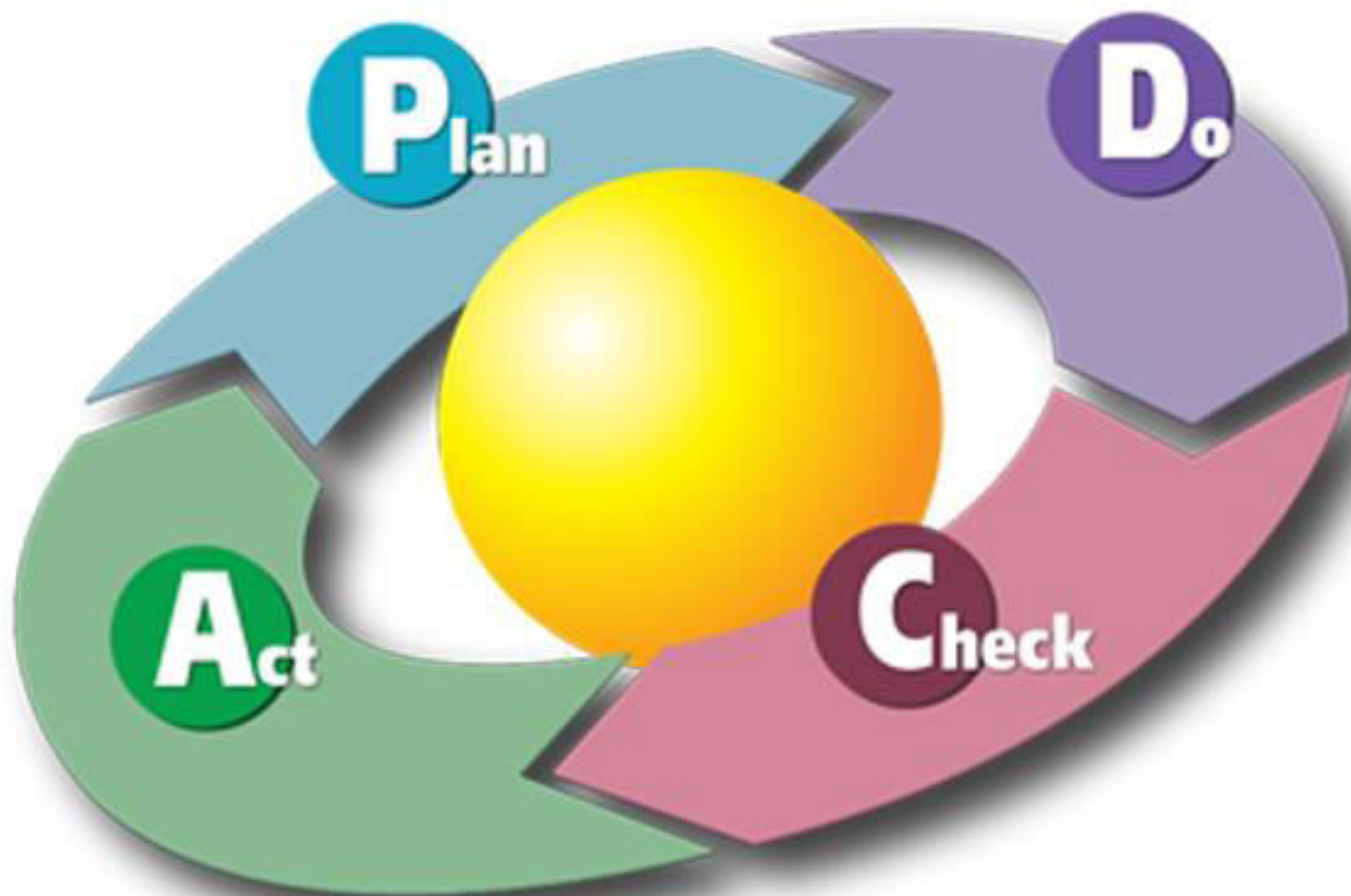
О чем стоит подумать

- Объем доработок в прикладных системах для их интеграции с IDM
- Организация интерфейса самообслуживания и процесса согласования заявок на доступ
- Управление учетными записями внештатных работников
- Учет системных и технологических учетных записей
- Управление учетными записями при наличии у сотрудника 2 и более учетных записей
- Перевод системы в контур интеграции IDM
- Обработка отпусков, декретного отпуска, больничных
- Замещение лиц, согласующих доступ

О чем стоит подумать

- Обработка событий со сменой наименования подразделений и должностей
- Перевод сотрудника внутри и между подразделениями
- Возможность оформление новых прав доступа, создание новых информационных ресурсов непосредственно в IDM
- Наличие необходимых отчетных форм
- Отзыв прав доступа (временно отсутствующим сотрудникам, отзыв прав непосредственным руководителем)
- Настройка взаимоисключающих привилегий
- Интеграция с системами аутентификации и SSO

Обеспечение ИБ – это правильно выстроенные процессы



Процесс управления правами доступа

ПЛАНИРОВАНИЕ:

Разработка Положения по организации доступа к информационным ресурсам, разработка проектной документации на внедрение IDM

ВНЕДРЕНИЕ:

Проведение мероприятий по реализации требований Положения. Внедрение IDM

КОНТРОЛЬ:

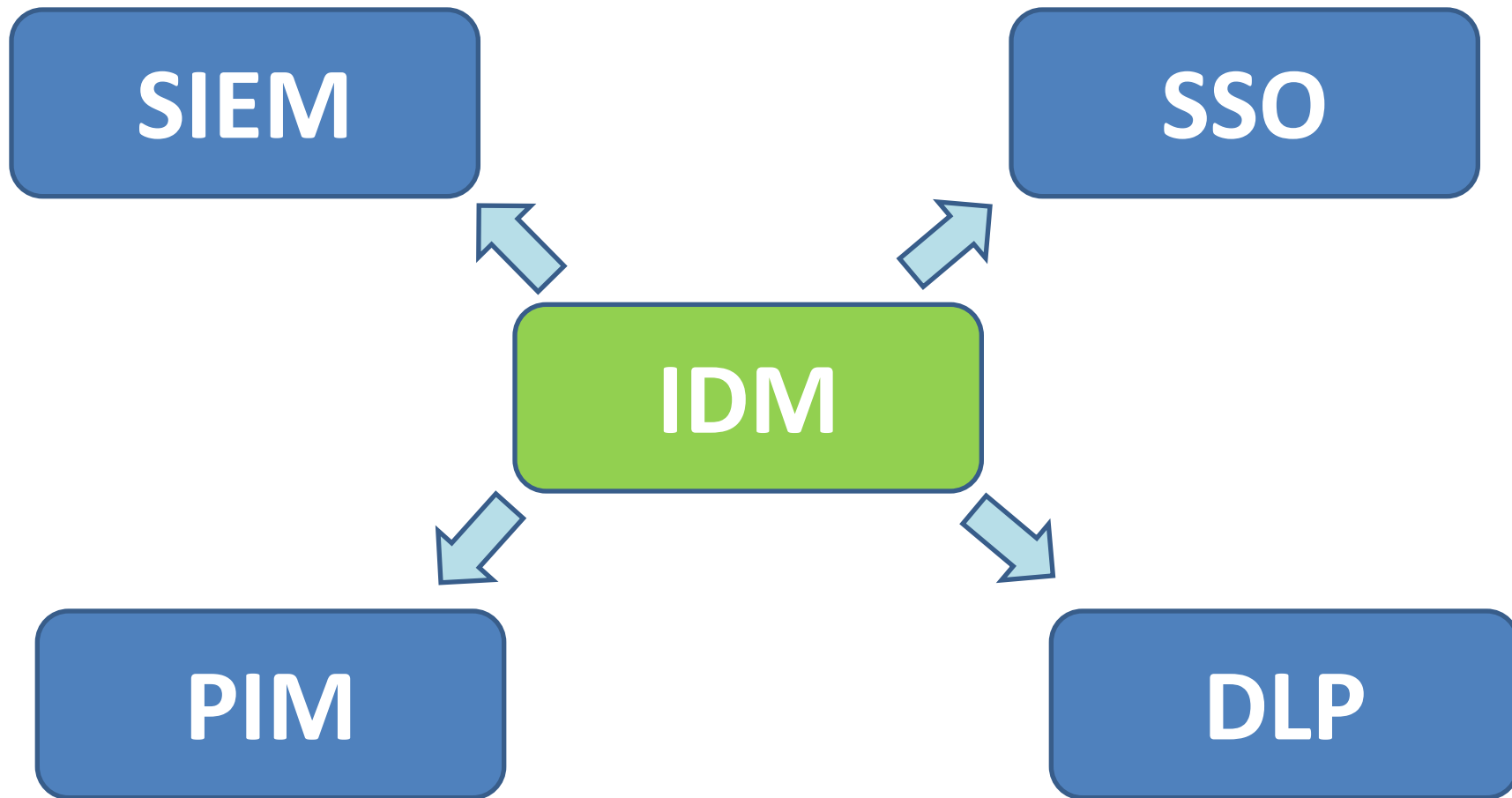
Текущий: участие в согласовании заявок на доступ к информационным ресурсам в IDM

Последующий: периодические внутренние проверки правомерности предоставления доступа, в том числе с использованием IDM; внешний аудит

СОВЕРШЕНСТВОВАНИЕ:

Внесение изменений в Положения по организации доступа к информационным ресурсам, разработка дополнительных инструкций, развитие IDM

Взаимодействие IDM другими продуктами по обеспечению ИБ



Мифы об IDM

- IDM обеспечивает контроль за действиями администраторов
- IDM отбирает у пользователей излишние права доступа
- Применение IDM позволяет реализовать принцип предоставления минимальных прав доступа





Банк высокой культуры

Скородумов Анатолий Валентинович

E-Mail: Skorodumov@mail.ru

Телефон (812) 329-50-64

Благодарю за внимание!