ЦЕНТР КИБЕРБЕЗОПАСНОСТИ

РОЛЬ СИСТЕМ КЛАССА IDM В ОПТИМИЗАЦИИ БИЗНЕС-ПРОЦЕССОВ

Андрей Каганский

Руководитель направления IDM-систем

sec.ussc.ru

Уральский центр систем безопасности (УЦСБ)

> 17
лет на рынке

> 1000
профессионалов в штате

> 2000
реализованных проектов

Топ-100 крупнейших отечественных ИТ-компаний [1]

Топ-15 крупнейших компаний России в сфере защиты информации [2]

Компетенции

- Информационная безопасность
- Информационные технологии
- Инженерно-технические средства охраны
- Анализ защищенности
- Центры обработки данных
- Умный дом
- Сервисный центр

[1] Рейтинг CNews100: Крупнейшие ИТ-компании России 2023
[2] Рейтинг CNews Security: Крупнейшие компании России в сфере защиты информации 2023

IDM-ПРОЕКТЫ

> 12
лет опыта
внедрения IDM

> 30
специалистов
в команде

> 30
реализованных
проектов

Отраслевой опыт

- Финансы и страхование
- Госсектор
- ИТ и телеком
- Энергетика
- Хим. промышленность
- Девелопмент
- Металлургия
- Нефтегазовый сектор
- Ритейл
- Финансовый сектор

СОДЕРЖАНИЕ

ПОЗИЦИОНИРОВАНИЕ И СОВРЕМЕННЫЕ ТЕНДЕНЦИИ

IDM как техническое средство – привычный подход

IDM как часть бизнес-инфраструктуры – современный подход

Роль консалтинга

Для успешной внедрения IDM необходим консалтинг на всех стадиях реализации проекта

Бизнес-процессы

Анализ БП компании,
Проектирование
обновленных
БП с учетом IDM

Управление рисками

Выявление рисковых
бизнес-операций,
формирование матриц
рисков, управление SoD

Организационные изменения

Преобразование / выделение
новых орг. подразделений,
штатных единиц,
функциональных ролей

Ролевая модель

Анализ ролей в системах,
формирование матриц
доступа и правил
назначения ролей с
учетом бизнес-операций
и функций

ПОДХОДЫ К ВНЕДРЕНИЮ

Драйверы внедрения IDM

Требования регуляторов

- **ГОСТ:** Р 57580.1-2017 (ЗИ)
- **ФЗ:** №149, 152, 187
- **Приказы ФСТЭК:** №17, 21, 31, 239
- **Указ Президента РФ:** №166

Автоматизация и оптимизация

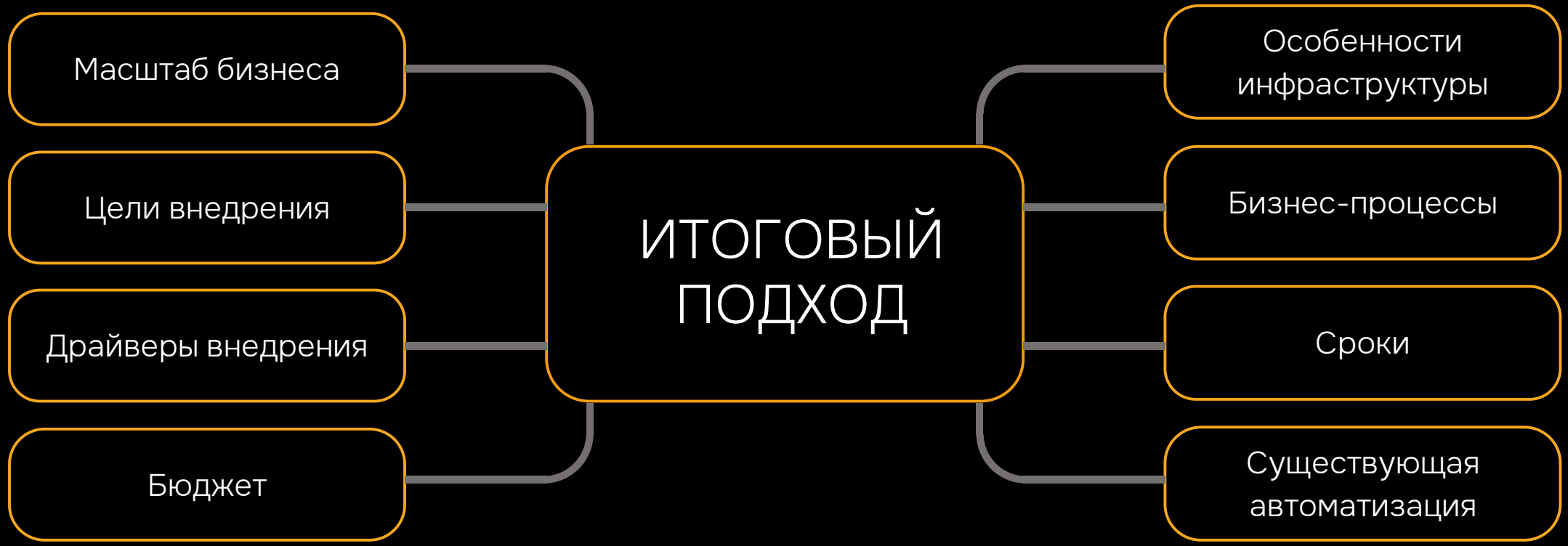
- Снижение операционных расходов
- Ускорение процессов
- Создание единого инструмента запроса, согласования и управления

Безопасность

- Снижение рисков утечек и компрометации
- Автоматизация блокировок
- Снижение риска человеческого фактора
- Контроль и аудит

Двух одинаковых IDM не бывает

Факторы, которые стоит учитывать при выборе подхода к внедрению



Привычный подход

«Техническое» внедрение

Акцент на автоматизации базовых процессов, интеграциях с информационными системами и ресурсами, выполнении рекомендаций стандартов и регуляторов и быстром получении первых результатов/эффектов

01
УМЕРЕННЫЙ БЮДЖЕТ

02
РЕЗУЛЬТАТЫ ЧЕРЕЗ 4-6 МЕС.

03
ЗАКРЫТИЕ БАЗОВЫХ ПОТРЕБНОСТЕЙ

Стадии реализация проекта

Фаза 1

ПИР

- Сбор исходных данных
- Анализ требований
- Техническое проектирование
- Проектирование бизнес-процессов
- Обследование интегрируемых систем

Фаза 2

Формирование «ядра» системы

- Интеграция с кадровым источником
- Интеграция с базовыми инфраструктурными сервисами
- Автоматизация ключевых процессов
- Запуск «ядра» в эксплуатацию

Фаза 3

Масштабирование

- Интеграция с информационными системами
- Автоматизация процессов
- Разработка эксплуатационной документации
- Поэтапный ввод в эксплуатацию

Фаза 4

Завершение проекта

- Устранение замечаний
- Проведение инструктажей
- Перевод системы в постоянную эксплуатацию

Расширенный подход

Создание глобальной среды

Помимо технического внедрение – формирование практик, подходов и методологии управления доступа, детальная комплексная проработка архитектуры, встраивание в бизнес-процессы компании, управление орг. изменениями

01
СТАНДАРТЫ И ЛУЧШИЕ ПРАКТИКИ

02
ЗАКРЫТИЕ ВСЕХ ПОТРЕБНОСТЕЙ

03
МАКСИМАЛЬНЫЙ ЭФФЕКТ ДЛЯ БИЗНЕСА

Стадии реализация проекта

ПРОЕКТНЫЙ ТРЕК | **ПРОЕКТНЫЕ ФАЗЫ**

	Предпроектный консалтинг	Инициация	Определение	Проектирование	Разработка	Тестирование	Развертывание	Завершение
БИЗНЕС-ПРОЦЕССЫ	Определение и утверждение: • Границ проекта • Стейкхолдеров и заинтересованных сторон • Функционального объема проекта • Требований • Зон ответственности м/у всеми участниками проекта	• Планирование проекта • Подготовка опросных листов для участников БП, владельцев БП, владельцев ИС, администратор-ов ИС • Подготовка инфраструктуры ландшафта разработки • Установка необходимых компонентов Системы • Проведение установочного совещания (kick off)	• Проведение интервью с вовлеченными категориями пользователей • Описание сценариев использования функций Системы • Утверждение состава технического проекта и архитектуры системы • Определение сценариев интеграции с каждой из ИС • Разработка частных технических заданий на интеграцию с каждой из • Разработка эскизного проекта Системы	Проектирование: • архитектуры Системы • функций Системы • интеграционных взаимодействий • бизнес-процессов, автоматизируемых Системой • глобального каталога ролей • матрицы доступа в ИС • матриц SoD-рисков	• Развертывание, установка и настройка тестового и продуктивного ландшафтов • Разработка и настройка коннекторов к ИС в границах цикла • Разработка и настройка бизнес-логики Системы (рабочие процессы, процессы согласования, обработчики событий и т.д.) • Разработка шаблонов отчетов • Загрузка матрицы доступа и правил назначения ролей в тестовый ландшафт • Подключение к ИС, загрузка данных • Разработка обучающих материалов • Разработка эксплуатационной документации	• Разработка документации для тестирования и предварительных испытаний Системы • Разработка плана миграции в продуктивный ландшафт Системы • Разработка программы ввода Системы в опытно-промышленную эксплуатацию • Разработка программы опытно-промышленной эксплуатации • Проведение предварительных испытаний в тестовом ландшафте Системы • Устранение замечаний по результатам тестирования	• Миграция конфигурации Системы в продуктивный ландшафт • Настройка подключения к продуктивным • Загрузка матрицы доступа и правил назначения ролей в продуктивный ландшафт • Подключение к ИС, загрузка данных • Ввод системы в ОПЭ • Мониторинг и сопровождение ОПЭ • Ведение журнала ОПЭ • Устранение замечаний по результатам ОПЭ • Проведение приемо-сдаточных испытаний Системы • Перевод Системы в промышленную эксплуатацию	Мониторинг работы Системы Разработка документации на техническое сопровождение Системы: • Программы гарантийной и технической поддержки • Регламента гарантийного обслуживания системы • Регламента гарантийного мониторинга системы Подписание закрывающих документов
ИНТЕГРАЦИИ								
РОЛЕВАЯ МОДЕЛЬ И РИСКИ								
ОРГ.ИЗМЕНЕНИЯ								

Time & Material

Разделение проекта на циклы

Подход, позволяющий совместить преимущества описанных ранее концепций, при этом дающий возможность гибко распоряжаться ресурсами и формировать требования на протяжении всего проекта

01
ГИБКИЕ СРОКИ

02
ФОРМИРОВНАИЕ ПОТРЕБНОСТИ «ЗДЕСЬ И СЕЙЧАС»

03
ОПТИМАЛЬНОЕ РАСПРЕДЕЛЕНИЕ РЕСУРСОВ

Стадии реализация проекта

Выбор подхода — основа успешного внедрения

Традиционный

+
- Быстрый результат
- Умеренный бюджет
- Возможность гибкого управления

−
- Фиксированный скоуп
- Ограниченный функционал

Расширенный

+
- Максимальный эффект для бизнеса
- Глубочайшая степень проработки
- Встраивание IDM в процессную модель

−
- Большой бюджет, долгие сроки
- Каскадная модель управления
- Требует значительных ресурсов и высокой квалификации исполнителей

Time &Material

+
- Возможность гибко управлять сроками и бюджетом
- Возможность оперативно подстраиваться под изменения в компании

−
- Сложнее с точки зрения управления
- Конечный результат отличается от запланированного
- Требует значительных ресурсов и высокой квалификации исполнителей

ОПИСАННЫЕ ПОДХОДЫ
НА ПРИМЕРЕ ПРОЕКТОВ УЦСБ

Пример №1:

традиционный подход

Крупное промышленное предприятие

> 15000 сотрудников

40 информационных систем

Срок реализации – 14 месяцев

Проектная команда – 5 тех. специалистов и РП

01. Четкие технические требования на старте, отсутствие консалтинга

Наличие четкого ТЗ дало возможность спланировать проект на начальной стадии и строго соблюдать план

02. Поэтапный ввод в эксплуатацию

Запуск ядра системы состоялся спустя 6 месяцев после старта проекта, Заказчик начал получать результат и знакомить пользователей с изменениями

03. Реализация базового функционала

Был выстроен фундамент, на базе которого Заказчик продолжает расширять функциональность

Пример №2:

расширенный подход

Крупное предприятие ТЭК

> 15000 сотрудников

12 информационных систем

Срок реализации – 26 месяцев

Результат в конце проекта

Проектная команда ~ 25 человек, включая архитекторов, инженеров, разработчиков, тестировщиков, бизнес и ИБ-аналитиков, консультантов, тренеров, РП

01. Проектирование и внедрение IAM-процессов

Заказчику необходим IDM не как техническая система, а как совокупность методик и подходов, позволяющих трансформировать бизнес-процессы компании и максимизировать выгоды бизнеса

02. Внедрение RBAC-модели и управления рисками

RBAC-модель позволяет на 80% автоматизировать процедуры управления ролями, модель управления рисками и SoD-конфликтами – свести к минимуму инциденты, вызванные злоупотреблением полномочиями

03. Консалтинг в части орг. изменений

Выделение новых функциональных ролей и подразделений в совокупности с обучением всех категорий пользователей на протяжении проекта позволяет эффективно внедрить новые процессы без ущерба для бизнеса

Пример №3:

T&M

Федеральный телеком-оператор

> 15000 сотрудников

> 100 информационных систем

Срок реализации – условно не ограничен

Результат в конце каждой фазы проекта

Проектная команда ~ 10 человек

01. Изначально планировался традиционный подход

На первой фазе было запущено ядро системы.
В виду специфики бизнеса инфраструктура и орг. структура Компании постоянно меняется, поэтому было принято решение перехода на T&M

02. Потребность в консалтинге по ходу проекта

Стремительный рост Компании, а также ряд внешних факторов сформировали потребность в пересмотре всей концепции управления доступом и построением единой экосистемы, ядром которой выступает IDM

03. Комплексный подход к управлению доступом

Разработана и продолжает разрабатываться ролевая модель в разрезе ОХД Компании, централизованно управляются и контролируются привилегированный доступ (в т.ч. в части критичных бизнес-операций) и аутентификационные данные

РЕКОМЕНДУЕМОЕ РЕШЕНИЕ

+ Ankey IDM

- Полностью отечественное IGA-решение
- Возможность переиспользования интеграционных, архитектурных и функциональных наработок внедренного решения при миграции
- Наличие доверенного партнера с опытом реализации аналогичных проектов
- Возможность функционирования в условиях технологического суверенитета
- Круглосуточная техническая поддержка от производителя, доступ к обновлениям, документации, базам знаний

Покрытие требований регуляторов:

- **Стандарт ГОСТ:** Р 57580.1-2017 (ЗИ)
- **ФЗ:** №149, 152, 187 (ЗИ, ИСПДн)
- **Указ Президента РФ:** №166 об обеспечении технологического суверенитета
- **Приказы ФСТЭК:** №17, 21, 31, 239
- **ISO 27001 / ГОСТ 27001:** контроль предоставления полномочий и их пересмотр
- **В реестре отечественного ПО**
- **Сертификат ФСТЭК №4107**
- **PCI DSS / СТО БР ИББС:** контроль создания, изменений и удаления данных ID, а также отзыв и пересмотр прав доступа

ЦЕНТР КИБЕРБЕЗОПАСНОСТИ

СПАСИБО ЗА ВНИМАНИЕ!
ВОПРОСЫ?

sec.ussc.ru

cybersec@ussc.ru

Андрей Каганский

Руководитель направления IDM-систем

akaganskiy@ussc.ru