NVisionGroup
ЭНВИЖН ГРУП
Динамичный интегратор

ПРЕДОТВРАЩЕНИЕ ИНСАЙДА – УПРАВЛЕНИЕ РИСКАМИ И БЕЗОПАСНОСТЬЮ

Касулин Юрий Сергеевич

Руководитель отдела систем контроля доступа
«Энвижн Груп»

NVisionGroup
ЭНВИЖН ГРУП

Содержание

«Лишний» доступ – причины и следствия

Ролевая модель – лекарство или тиски

«Таблетки» или «Лечение». Подходы, используемы при построении ролевой модели

NVisionGroup
ЭНВИЖН ГРУП

«Лишний» доступ: причины и следствия

Большое количество банковских ИС и пользователей приводит к тому, что не всегда можно отследить **избыточность прав** доступа пользователей к данным.

Избыточные права доступа могут привести к утечке информации и, как следствие, к **мошенническим действиям.**

NVisionGroup
ЭНВИЖН ГРУП

Ситуация №1: Выдача кредита

Возможность повлиять на одобрение кредитной заявки

Кредитный консультант, при наличии доступа к результатам скоринга, может повлиять на решение банка выдать кредит потенциальному заемщику

Отсутствие строгого контроля прав доступа

Ситуация №2: Совмещение должностей

Избыточный доступ к информационным системам

При совмещении обязанностей (даже временном), сотрудник банка может получить избыточный доступ к операциям и данным из АБС.

Не отслеживаются конфликты полномочий

NVisionGroup
ЭНВИЖН ГРУП

Ситуация №3: Сговор с администратором системы

Действия группы лиц

Администратор АБС может предоставить избыточные права доступа определенным сотрудникам банка.

Отсутствует контроль процессов
назначения прав и избыточности полномочий

Ролевая модель – лекарство или тиски

Одно из условий неизбыточности прав доступа к ИС – создание и поддержка актуальной **ролевой модели**

Ролевая модель включает в себя:

- Каталог информационных ресурсов
- Каталог технических ролей доступа к информационным ресурсам
- Каталог типовых (бизнес) ролей и их соответствия ролям доступа
- Каталог соответствия бизнес ролей организационным единицам

Построение ролевой модели доступа с нуля

Задача бизнес-подразделения	Определение функциональных обязанностей типовой должности (бизнес роли)
Задача системного аналитика	Определение прав и полномочий типовой должности в АС*
Задача ИТ-службы	Настройка технических ролей доступа к АС

* - Автоматизированная система

NVisionGroup
ЭНВИЖН ГРУП

Поддержка ролевой модели

Ролевая модель должна всегда быть актуальной и соответствовать фактическим правами доступа пользователей

Администрирование ролевой моделью должно быть простым и прозрачным

Автоматизация управления ролевой моделью

решение класса Role Management

NVisionGroup
ЭНВИЖН ГРУП

Преимущества внедрения автоматизированного решения

- Единое хранилище информации об информационных ресурсах, технических ролях, бизнес-ролях и правах доступа конечных пользователей
- Созданная структура данных наглядна и удобна для администрирования и аудита
- Стандартизированные процессы управления ролями и доступом пользователей
- Ограничение доступа к конфиденциальной информации
- Выявление избыточности полномочий пользователей через настройку правил SoD (Segregation of Duties)

Коробочные решения

Внедрение готового продукта от ведущего вендора

ORACLE

IBM

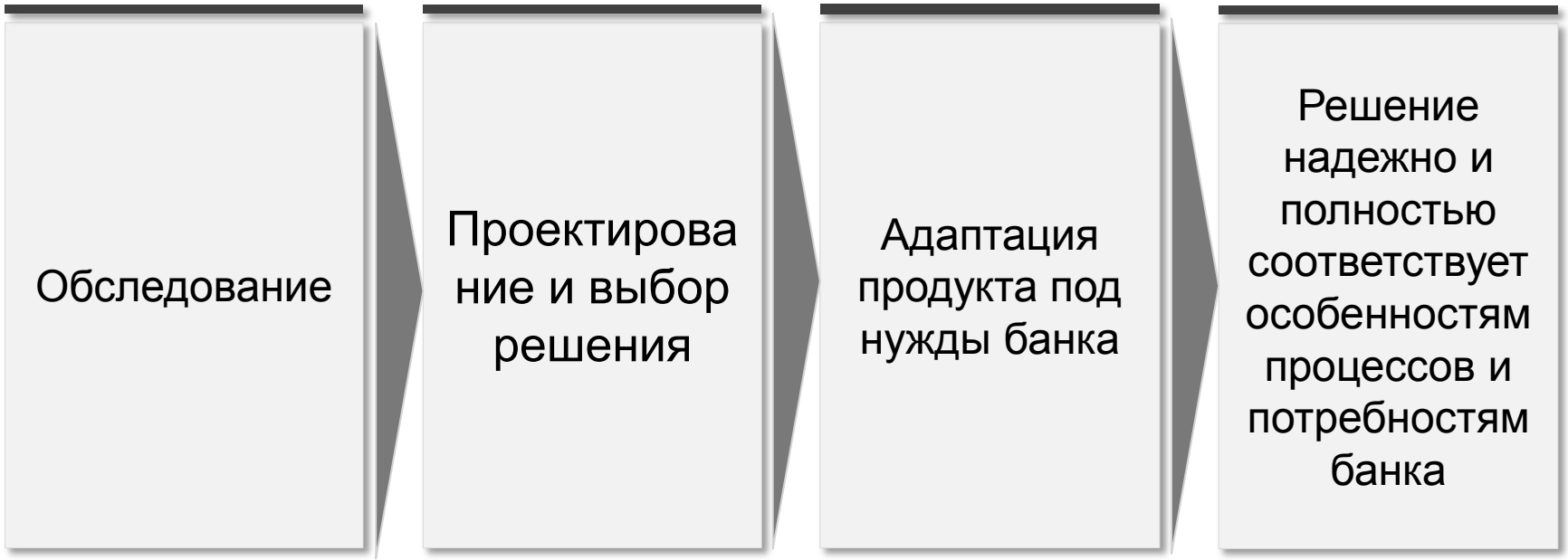
Avanpost

Trustverse

- Универсальное решение
- Соответствие стандартам ИБ
- НО! Возможно несоответствие потребностям банка

NVisionGroup
ЭНВИЖН ГРУП

Комплексный подход



Обследование и проектирование – залог успешного внедрения

- Обследование и анализ процессов управления ролями и доступом «как есть», анализ ИТ-инфраструктуры организации
- Определение границ проекта: организационные границы, доверенные источники данных, целевые системы
- Разработка концепции решения и выбор продукта
- Разработка сценариев работы системы и модели данных
- Проектирование системы
- Планирование внедрения

Ситуация №1: Выдача кредита

Возможность повлиять на одобрение кредитной заявки

Кредитный консультант не сможет повлиять на результаты скоринга

Полномочия строго ограничены

Ситуация №2: Совмещение должностей

Избыточный доступ к информационным системам

При совмещении обязанностей (даже временном), сотрудник банка не сможет получить избыточный доступ к операциям и данным из АБС.

Конфликты полномочий пользователей (SoD) отслеживаются и предотвращаются даже при работе под несколькими учетными записями

Ситуация №3: Сговор с администратором системы

Действия группы лиц

Администратор АБС не сможет предоставить избыточные права доступа без риска быть вычисленным.

Полномочия администраторов по управлению правами доступа пользователей минимизированы и отслеживаются

Касулин Юрий Сергеевич

Руководитель отдела систем контроля доступа

Центральный офис

Россия, 115054, Москва, ул. Дубининская, д.53, стр.5

Тел.: +7 (495) 641-12-12

Факс: +7 (495) 641-12-11

www.nvg.ru

NVisionGroup

ЭНВИЖН ГРУП

Динамичный интегратор