КОНТРОЛЬ ДОСТУПА К ИНФОРМАЦИОННЫМ РЕСУРСАМ

Павлова Ксения, CISA, CISM

ПЛАН ПРЕЗЕНТАЦИИ

- Предпосылки создания системы
- Примеры инцидентов информационной безопасности
- Решение инцидентов
- Функционал и возможности системы
- Архитектура системы

ПРЕДПОСЫЛКИ СОЗДАНИЯ СИСТЕМЫ ФОРМИРОВАНИЯ МАТРИЦЫ ДОСТУПА

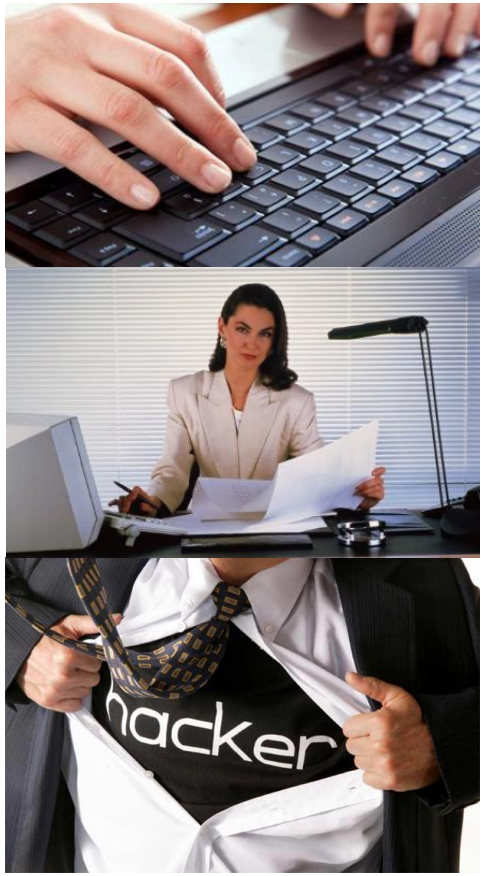
- Контроль доступа к защищаемой информации

- Снижение вероятности возникновения инцидентов

- Сбор информации для расследования инцидентов

ПРИМЕР 1. ПРЕДОСТАВЛЕНИЕ ПРАВ ДОСТУПА

- Сотруднику для выполнения новой задачи требуется предоставить доступ и/или повысить привилегии
- Руководитель структурного подразделения заинтересован в выполнении задачи и согласовывает заявку
- Специалисты по ИБ – не имеют инструмента для проверки допустимости совмещения требуемых привилегий с уже существующими
- Сотрудник накапливает критический объем привилегий



ПРИМЕР 1. РЕШЕНИЕ

1. При назначении прав доступа необходимо иметь инструмент для анализа существующих прав доступа пользователя

2. Новые права доступа должны предоставляться только если в совокупности с существующими правами доступа не создаются предпосылки для возникновения инцидентов

Результаты

- Специалисты по ИБ получат основания для согласования / отказа назначения новых прав доступа
- Снижение вероятности возникновения инцидентов

ПРИМЕР 2. КОНТРОЛЬ ПРАВ ДОСТУПА

- Главный бухгалтер проводит периодический контроль за распределением прав доступа в 1С
- Для контроля избыточности прав главный бухгалтер запрашивает справку о распределении прав доступа
- Специалисты ИТ представляют неактуальную справку
- При возникновении инцидента (кража информации) круг подозреваемых неактуален

ПРИМЕР 2. РЕШЕНИЕ

1. Необходима возможность автоматического сравнения текущих прав доступа с согласованным эталоном
2. Матрицу доступа должна предоставляться в удобном для восприятия виде
3. Все изменения в матрицу доступа должны согласовываться с владельцем ресурса

Результаты

- Владелец ресурса и специалист по ИБ всегда могут получить актуальную матрицу доступа
- Регламентированный процесс предоставления прав доступа

ПРИМЕР 3. ИЗМЕНЕНИЕ ОБЯЗАННОСТЕЙ СОТРУДНИКА

- Сотрудника перевели из одного отдела в другой
- Сотруднику были выделены новые права доступа
- Старые права доступа не были аннулированы
- Произошел инцидент - база данных была украдена
- При расследовании инцидента данного сотрудника никто не заподозрил, т.к. его текущие обязанности не предполагают доступ к базе

ПРИМЕР 3. РЕШЕНИЕ

1. Отдел кадров должен информировать специалистов ИБ об изменениях в штатном расписании
2. Специалисты ИБ и бизнес-подразделений должны анализировать текущие права доступа на предмет их необходимости для выполнения новых должностных обязанностей
3. Необходимо аннулировать все не требуемые права доступа

Результаты

- Регламентированный процесс предоставления прав доступа
- Снижение вероятности возникновения инцидентов

ПРИМЕР 4. КРАЖА ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ

- Сотрудник легально работал с защищаемой информацией
- При этом сотрудник сделал копии защищаемой информации и уволился
- Факт кражи защищаемой информации был обнаружен не сразу
- Не смогли определить виновника, т.к. не знали, кто имел доступ к системе на момент инцидента

ПРИМЕР 4. РЕШЕНИЕ

1. Необходима возможность хранения нескольких согласованных эталонов прав доступа

2. Необходима возможность автоматического сохранения текущих правил доступа для последующего анализа (по расписанию)

Результаты

- Можно восстановить актуальную матрицу доступа на требуемую дату
- Получение оснований для включения сотрудников в список возможных источников в инцидента

ПОЧЕМУ ВСЕ ЭТО ПРОИЗОШЛО?

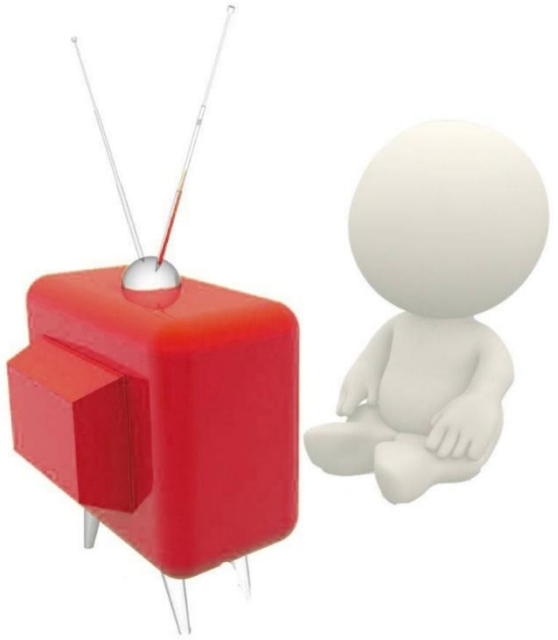
- Отсутствие текущей картины разграничения прав доступа
- Отсутствие возможности контроля соответствия текущих прав доступа согласованным
- Отсутствие истории изменений прав доступа

ТРЕБОВАНИЯ К УПРАВЛЕНИЮ ДОСТУПОМ К КТ

1. Наличие автоматизированного инструмента для анализа текущих прав доступа
2. Предоставление информации для владельца ресурса и сотрудника ИБ в понятном виде
3. Возможность создания согласованного эталона прав доступа
4. Возможность сравнения текущих прав доступа с согласованным эталоном
5. Ведение истории изменения прав доступа
6. Регламентация процесса предоставления, изменения и отзыва прав доступа

ФУНКЦИОНАЛ. «ЖИВЫЕ» ПРИМЕРЫ

- Анализ текущих прав доступа конкретного сотрудника
- Формирование матрицы доступа для ресурса
- Сравнение текущих прав доступа с согласованным эталоном
- Хранение истории изменения прав доступа



АНАЛИЗ ТЕКУЩИХ ПРАВ ДОСТУПА КОНКРЕТНОГО СОТРУДНИКА

Ресурсы | Версии | Отчет № 89

Обновить | Сохранить | Сравнить

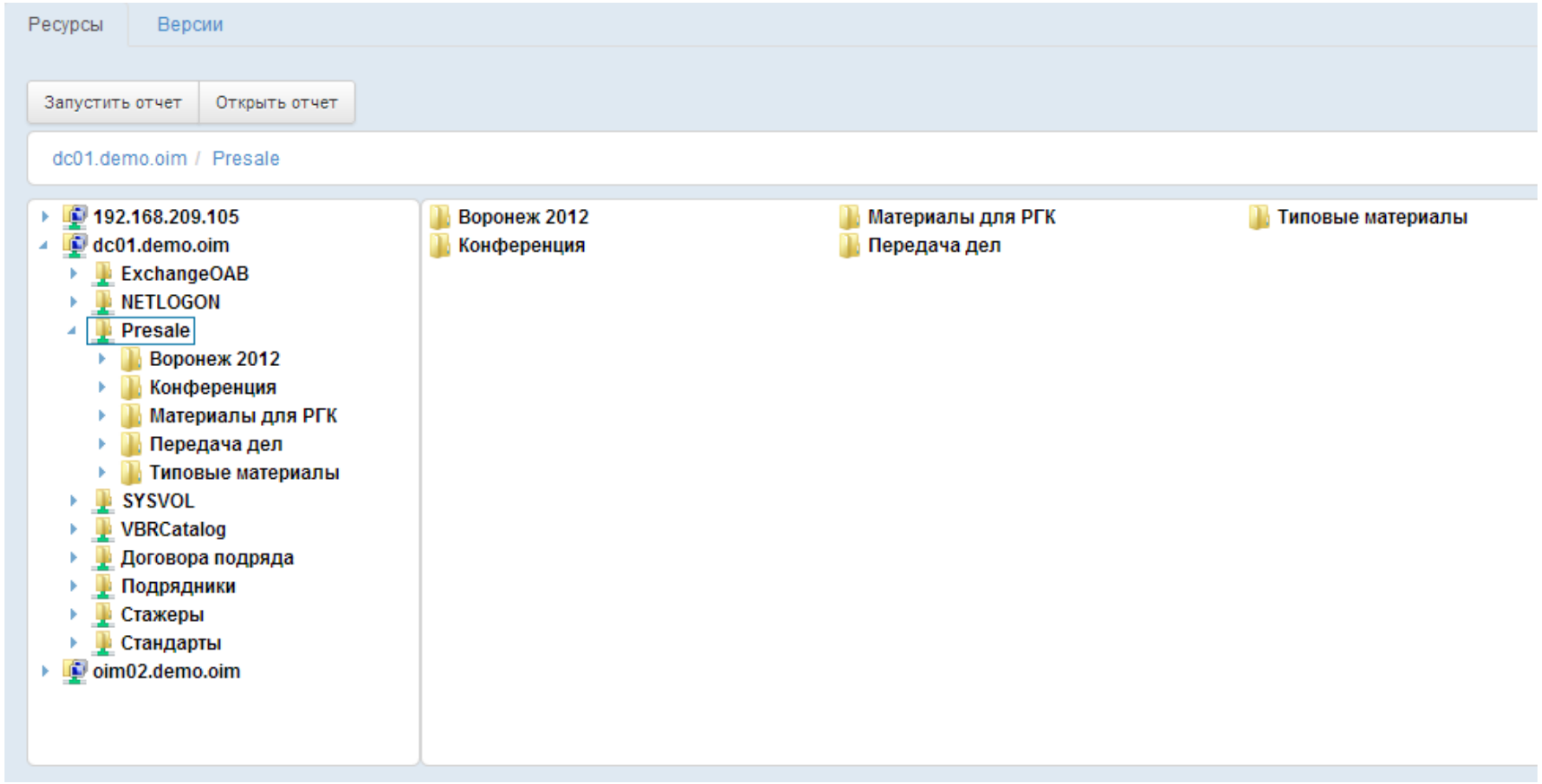
demo\smirnov.andrey

Объект	Субъект	Применять к	Полный доступ	Изменение	Чтение	Запись
\\dc01.demo.oim\Presale	DEMO\smirnov.andrey		☐	☐	☑	☐
\\dc01.demo.oim\Presale	DEMO\smirnov.andrey	Для этой папки и ее подпапок и файлов	☐	☐	☑	☐
\\dc01.demo.oim\Presale\Конференция	DEMO\smirnov.andrey	Для этой папки и ее подпапок и файлов	☑	☑	☑	☑
\\dc01.demo.oim\Presale\Конференция	DEMO\smirnov.andrey	Унаследовано. Для этой папки и ее подпапок и файлов	☐	☐	☑	☐
\\dc01.demo.oim\Presale\Материалы для РГК	DEMO\smirnov.andrey	Для этой папки и ее подпапок и файлов	☐	☐	☑	☐
\\dc01.demo.oim\Presale\Передача дел	DEMO\smirnov.andrey	Для этой папки и ее подпапок и файлов	☑	☑	☑	☑
\\dc01.demo.oim\Presale\Передача дел	DEMO\smirnov.andrey	Унаследовано. Для этой папки и ее подпапок и файлов	☐	☐	☑	☐
\\dc01.demo.oim\Presale\Типовые материалы	DEMO\smirnov.andrey	Унаследовано. Для этой папки и ее подпапок и файлов	☐	☐	☑	☐
\\dc01.demo.oim\Presale\Типовые материалы\Буклеты и ...	DEMO\smirnov.andrey	Унаследовано. Для этой папки и ее подпапок и файлов	☐	☐	☑	☐
\\dc01.demo.oim\Presale\Типовые материалы\Буклеты и ...	DEMO\smirnov.andrey	Унаследовано. Для этой папки и ее подпапок и файлов	☐	☐	☑	☐
\\dc01.demo.oim\Presale\Типовые материалы\Буклеты и ...	DEMO\smirnov.andrey	Унаследовано. Для этой папки и ее подпапок и файлов	☐	☐	☑	☐
\\dc01.demo.oim\Presale\Типовые материалы\Буклеты и ...	DEMO\smirnov.andrey	Унаследовано. Для этой папки и ее подпапок и файлов	☐	☐	☑	☐
\\dc01.demo.oim\Presale\Типовые материалы\Буклеты и ...	DEMO\smirnov.andrey	Унаследовано. Для этой папки и ее подпапок и файлов	☐	☐	☑	☐
\\dc01.demo.oim\Presale\Типовые материалы\Буклеты и ...	DEMO\smirnov.andrey	Унаследовано. Для этой папки и ее подпапок и файлов	☐	☐	☑	☐
\\dc01.demo.oim\Presale\Типовые материалы\Буклеты и ...	DEMO\smirnov.andrey	Унаследовано. Для этой папки и ее подпапок и файлов	☐	☐	☑	☐
\\dc01.demo.oim\Presale\Типовые материалы\Буклеты и ...	DEMO\smirnov.andrey	Унаследовано. Для этой папки и ее подпапок и файлов	☐	☐	☑	☐

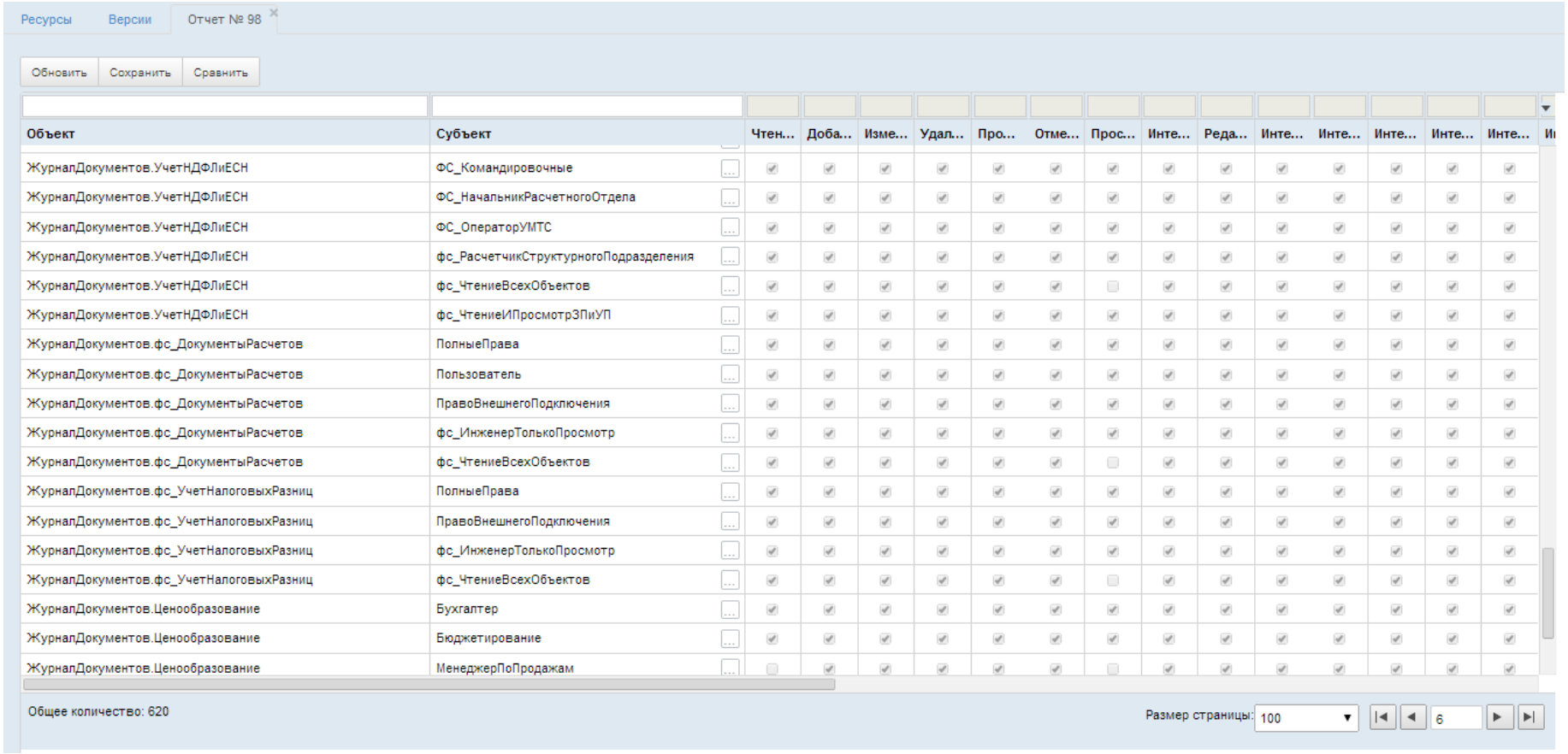
Общее количество: 86

Размер страницы: 25 | 1

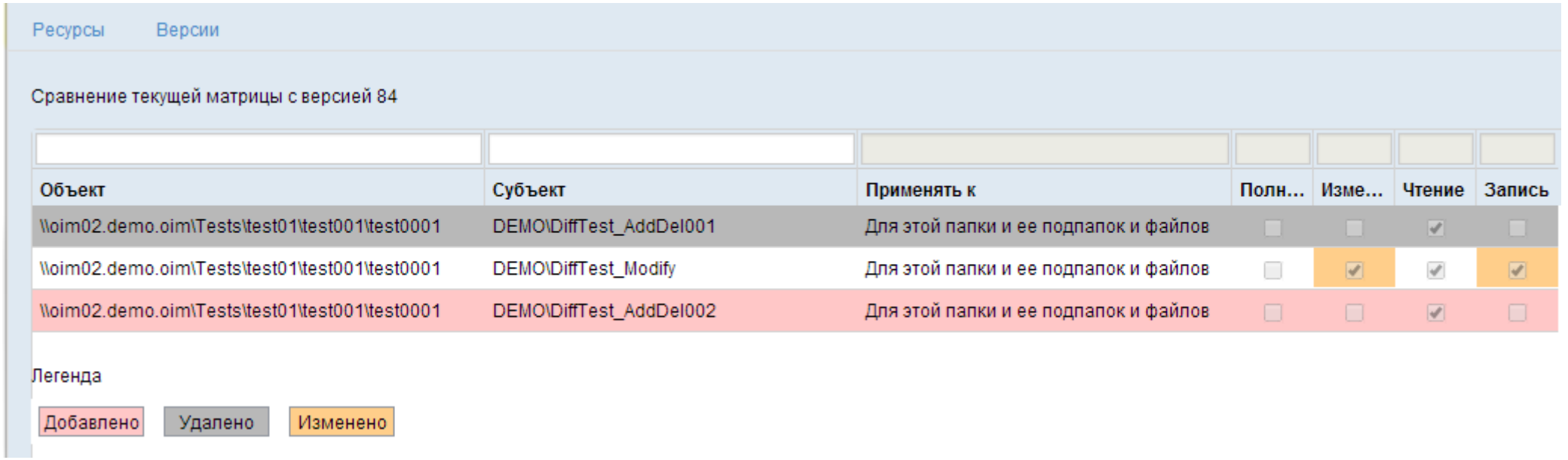
ФОРМИРОВАНИЕ МАТРИЦЫ ДОСТУПА ДЛЯ РЕСУРСА



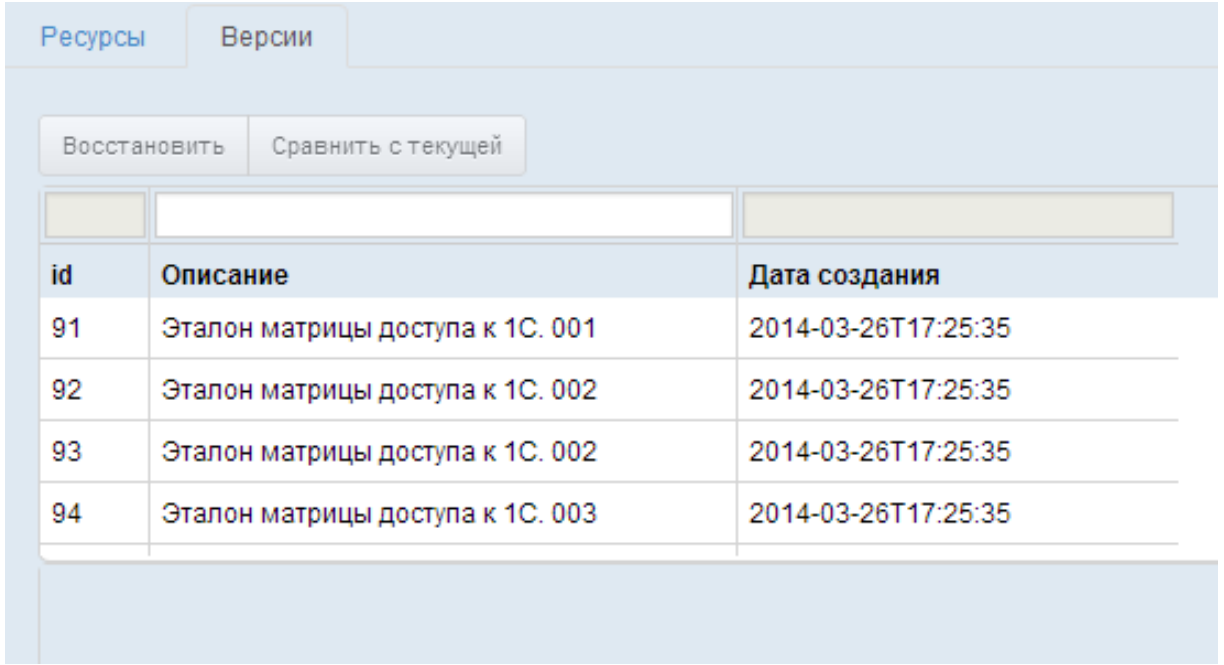
ФОРМИРОВАНИЕ МАТРИЦЫ ДОСТУПА ДЛЯ РЕСУРСА



СРАВНЕНИЕ ТЕКУЩИХ ПРАВ ДОСТУПА С ЭТАЛОНОМ



ХРАНЕНИЕ ИСТОРИИ ИЗМЕНЕНИЯ ПРАВ ДОСТУПА



id	Описание	Дата создания
91	Эталон матрицы доступа к 1С. 001	2014-03-26T17:25:35
92	Эталон матрицы доступа к 1С. 002	2014-03-26T17:25:35
93	Эталон матрицы доступа к 1С. 002	2014-03-26T17:25:35
94	Эталон матрицы доступа к 1С. 003	2014-03-26T17:25:35

ПРЕИМУЩЕСТВА ИСПОЛЬЗОВАНИЯ СИСТЕМЫ ФОРМИРОВАНИЯ МАТРИЦЫ ДОСТУПА

- Повышение эффективности работы сотрудников ИБ
- Возможность оперативного предоставления информации для расследования инцидентов
- Необходимость наличия удобного инструмента для автоматического мониторинга текущих прав доступа

СПАСИБО ЗА ВНИМАНИЕ!

Вопросы?

ОБЪЕКТЫ И ПРИНЦИПЫ ЗАЩИТЫ

Перечень объектов защиты:

- СУБД: Oracle Database и Microsoft SQL
- ERP-системы на базе «1С» и «Axapta»
- Файловые ресурсы Windows и Unix