



КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ



26 апреля 2018 г.
г. Санкт-Петербург

#CODEIB

IDENTITY GOVERNANCE 360°. В ЧЕМ ЦЕННОСТЬ IDM-РЕШЕНИЙ?



ГАЗИНФОРМСЕРВИС

www.gaz-is.ru

РОМАН ЛУНЁВ

Ведущий менеджер
ГАЗИНФОРМСЕРВИС

EMAIL: Lunev-R@gaz-is.ru

89%

уволенных сотрудников
сохраняют доступ к
системам и почте

43%

получение доступа
занимает недели и
месяцы

22%

получение
доступа занимает
минуты и часы

71%

имеют доступ к
корпоративным данным,
видеть которые им не
положено

54%

пользуются
избыточным
доступом часто
или очень часто

38%

могут получить доступ
к «множеству данных»

Служба ИБ

- Избыточные права
- Бесхозные учетные записи
- Отсутствие архивных данных

Служба ИТ

- Большой поток заявок на доступ
- Множество пользователей
- Отсутствие синхронизации

Бизнес-пользователи

- Множество учетных записей
- Множество паролей
- Длительное время ожидания доступа



Утечка
конфиденциальной
информации



Простои
сотрудников



Высокие
издержки

09.09.2015

ОСУЖДЕН БЫВШИЙ СОТРУДНИК «АЛЬФАСТРАХОВАНИЕ», ПОХИТИВШИЙ ДЛЯ ПРОДАЖИ БАЗУ ДАННЫХ КЛИЕНТОВ

Весной 2014 года бывший сотрудник «АльфаСтрахование», используя рабочий доступ к информационным системам компании, скопировал из них информацию о договорах страхования, заключенных с ОАО «АльфаСтрахование». Впоследствии полученную незаконным путем базу данных он передал посреднику для дальнейшей перепродажи.

Благодаря совместным действиям службы экономической безопасности «АльфаСтрахование» и ГУ МВД России по г. Москве все участники противоправного деяния были задержаны. Было возбуждено уголовное дело по статье «Незаконное разглашение сведений, составляющих коммерческую тайну».

В августе 2015 года Лефортовский районный суд г. Москвы рассмотрел материалы дела и признал бывшего сотрудника «АльфаСтрахование», осуществившего похищение данных, виновным в совершении преступления, предусмотренного ч.3 ст. 193 УК РФ («Незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну»), и назначил ему наказание в виде лишения свободы сроком на два года (условно).

Обиженный сисадмин после увольнения удалил на бывшей работе четырёхлетний архив бухучёта

9 апреля Заводский районный суд г. Кемерово вынес приговор в отношении 32-летнего бывшего ведущего специалиста информационных технологий Алексея Приходько, который был признан виновным в неправомерном доступе к охраняемой компьютерной информации, повлекшем её уничтожение (ч.1 ст. 272 УК РФ).



В июле 2011 года Приходько зашёл на почтовый сервер предприятия, где он ранее работал, и удалил программу «1С Предприятие» за период с 2007 по 2011 год.

В результате данные бухгалтерского учёта на серверах трёх прокопьевских организаций крупной кузбасской холдинговой компании, на которую Приходько работал около года, были уничтожены.

Учитывая то, что сисадмин ранее судимостей не имел, суд назначил Приходько наказание в виде полугода исправительных работ условно с испытательным сроком 6 месяцев.






Система обеспечивает
**централизованное управление
идентификационными данными и
правами доступа**

Кто имеет доступ?

Кто должен иметь доступ?

Как этот доступ используется?

GIS  Ankey Identity Manager USER0005 

Мои заявки 

Номер	Название	Создана	Статус
6	Назначение ролей	05.02.2018 15:40	<input type="radio"/> На согласовании


Заявка № 6 от 05.02.2018

Информация

Этап согласования

Название этапа	Прямой руководитель
Согласующий	Петров Пётр Петрович

Запрашиваемые роли (3)

- Системно-техническая инфраструктура 
- Файловый ресурс кадровой службы
- Удаленный доступ
- Мобильная связь

Форма заявки

Обоснование	Служебная необходимость
Договор КТ	13 от 21.01.2018

The screenshot displays the Ankey Identity Manager web interface. On the left is a dark blue sidebar with navigation items: 'Входящие', 'Мои заявки', 'Мой профиль', 'Пользователи', 'Роли', 'Подразделения', 'Инф. системы', and 'Админ. системы'. The 'Админ. системы' item is expanded to show 'Периодические задания'. The main content area is titled 'Ankey Identity Manager' and 'Периодические задания'. It features a search bar, a refresh button, and a table of tasks.

Название	Последний запуск	Включена
ADGroupLookupRecon	Успешно (минуту назад)	Вкл
ADOrgLookupRecon	Успешно (минуту назад)	Вкл
ADUserRecon	Успешно (несколько секунд наза)	Вкл
ADUserSyncRecon	Успешно (несколько секунд наза)	Вкл
clearpasswordhistorytask	Не выполнялась	Вкл
csvorgreconjob	Успешно (несколько секунд наза)	Вкл
csvuserreconjob	Успешно (несколько секунд наза)	Вкл
evaluate	Успешно (минуту назад)	Вкл
failedsync	Успешно (несколько секунд наза)	Вкл
workflowrequest	Успешно (несколько секунд наза)	Вкл

jaspersoft: MongoDB Repo x

localhost:8080/jasperserver-pro/flow.html?_flowId=viewReportFlow&standAlone=true&_flowId=viewReportFlow&ParentFolderUri=%2Fpublic%2FMongoDB%2...

JASPERSOFT Library View Manage Create superuser | Help | Log Out

MongoDB Report Data refreshed Dec 1, 2013 at 4:30:46 PM

Requests Per Day

Legend: # Cases (blue), # Cases pending (red), # Cases closed (green), # Cases open (purple)

5 Oldest Requests

Status	Last Status	Case Age
Open Cases 1654 ▼	null	02-Dec -12
Closed Cases 1664 ▲	null	02-Dec -12
Pending 1676 ▼	pending	02-Dec -12
	closed	02-Dec -12
	closed	02-Dec -12

Requests by Service

About JasperReports Server Copyright © 2000-2013 Jaspersoft Corporation

Основные задачи

СНИЖЕНИЕ
накладных расходов

КОНТРОЛЬ
учётных записей

ОПТИМИЗАЦИЯ
рабочего времени

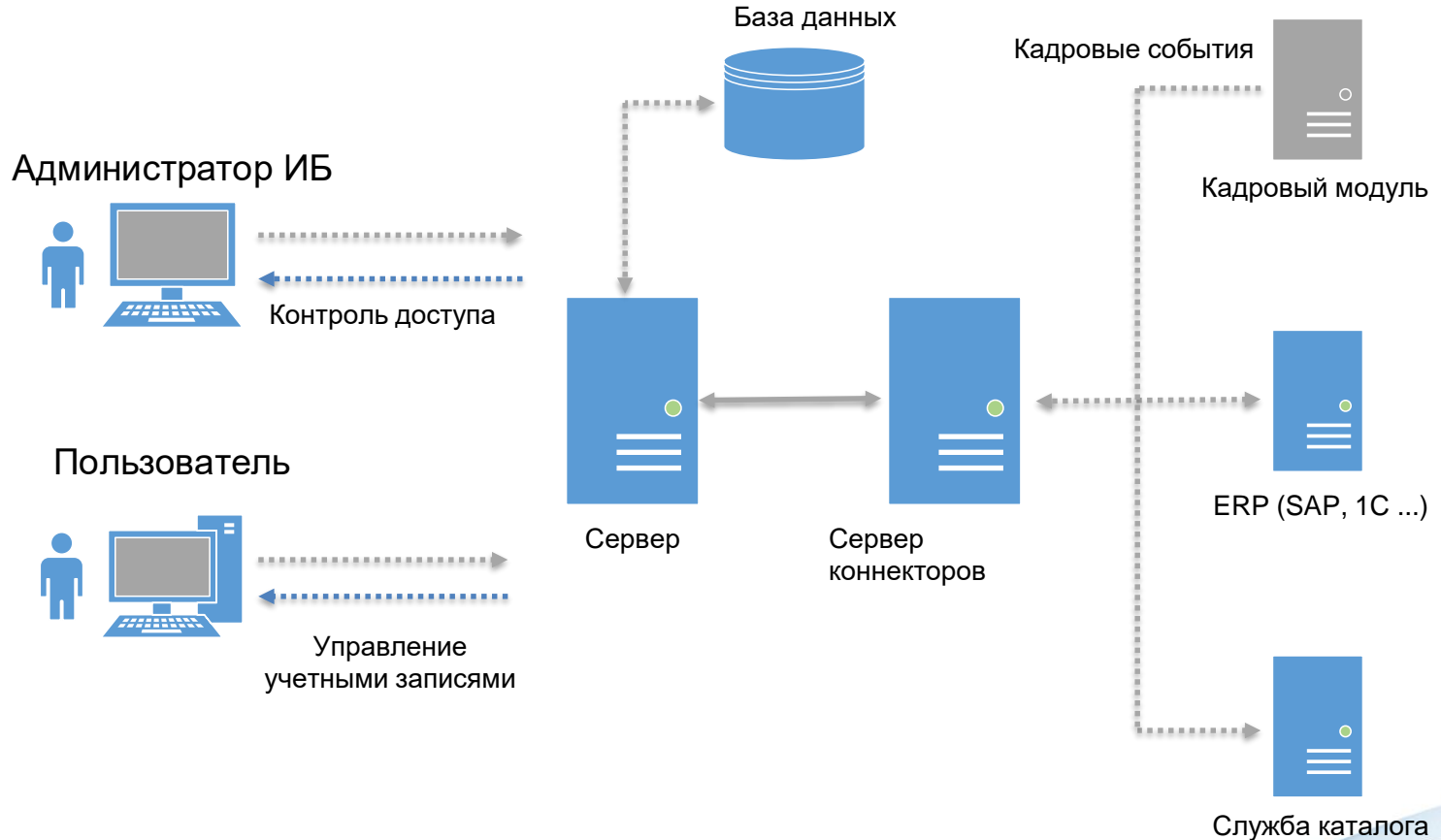


КОНТРОЛЬ
обмена данными

РАЗГРАНИЧЕНИЕ
обязанностей

ОПТИМИЗАЦИЯ
предоставления
доступа

Архитектура



Функциональные модули



Сценарии IdM/IAM

- Прием/перевод/увольнение сотрудника
- Длительный отпуск и делегирование доступа
- Управление доступом и разрешениями на основании бизнес-ролей
- Заявки на расширенный доступ и согласование через портал самообслуживания
- Изменения в обход системы
- Кто и куда имеет доступ? Почему?

Сценарии IGA

- Разделение полномочий.
- Построение ролевой модели
- Плановая аттестация прав доступа владельцами систем
- Агрегирование и управление информацией о сотруднике в информационных системах
- Сбор информации для аудита.
- Отчетность

Выгоды от использования IDM

Автоматизация
процессов и аналитика

Снижение риска
утечки информации

Ролевая модель
доступа

Отчеты о правах
пользователей

Оперативная
блокировка доступа



Зарубежные

- Защита от санкций
- Лояльная разработка
- Низкая стоимость
- Русскоязычная поддержка

Отечественные

- Производительность и отказоустойчивость
- Независимость от иностранного коммерческого ПО
- Разработка коннекторов на OpenICF
- Низкая стоимость владения и простота сопровождения

Road Map 2018

Управление
ресурсами

Сертификация
доступа

Заявка на роль

Консолидация
полномочий



Сертификация
ФСТЭК

Электронная
заявка

Разграничение
полномочий

Консолидация
ролей

Пример внедрения

Пользователи: 1 500

Информационные системы:

- 5 типовых   Exchange  SharePoint  Active Directory 
- 3 нетиповых АСМО  

Стоимость:

- Лицензии: 8,1 млн. ₺
- Внедрение: 12 млн. ₺ (8 месяцев)
- Оборудование: 3 млн. ₺

Обслуживание в год: 2 млн. ₺

Расходы на управление учётными записями в год: 9,2 млн. ₺

Текущее кадровое управление, аудит прав доступа, обработка заявок на изменение прав доступа, смену паролей

ROI составил 26% по итогам 4-х лет эксплуатации системы



Вы можете получить:

- Демоверсию **Ankey IDM**
- Бесплатную консультацию
- Пилотное внедрение

Более подробную информацию о продукте Вы найдете, перейдя по ссылке:

<http://www.gaz-is.ru/ankey-idm>





КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ



26 апреля 2018 г.
г. Санкт-Петербург

#CODEIB



ГАЗИНФОРМСЕРВИС

www.gaz-is.ru

РОМАН ЛУНЁВ

Ведущий менеджер
ГАЗИНФОРМСЕРВИС

EMAIL: Lunev-R@gaz-is.ru