

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

ВСЁ ПОД КОНТРОЛЕМ: безопасность начинается с корректных прав



ДМИТРИЙ БОНДАРЬ

РУКОВОДИТЕЛЬ
НАПРАВЛЕНИЯ INRIGHTS,
SOLAR SECURITY

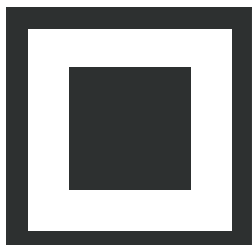
КОНТАКТЫ

ТЕЛ. +7 (499) 755-07-07
d.bondar@solarsecurity.ru

#CODEIB



Г. НОВОСИБИРСК
10 СЕНТЯБРЯ 2015

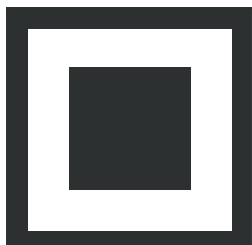


ИЗМЕНЕНИЕ ОБЪЁМА ФИНАНСОВЫХ УБЫТКОВ В РЕЗУЛЬТАТЕ ИНЦИДЕНТОВ ИБ

В мире, 2013-2014

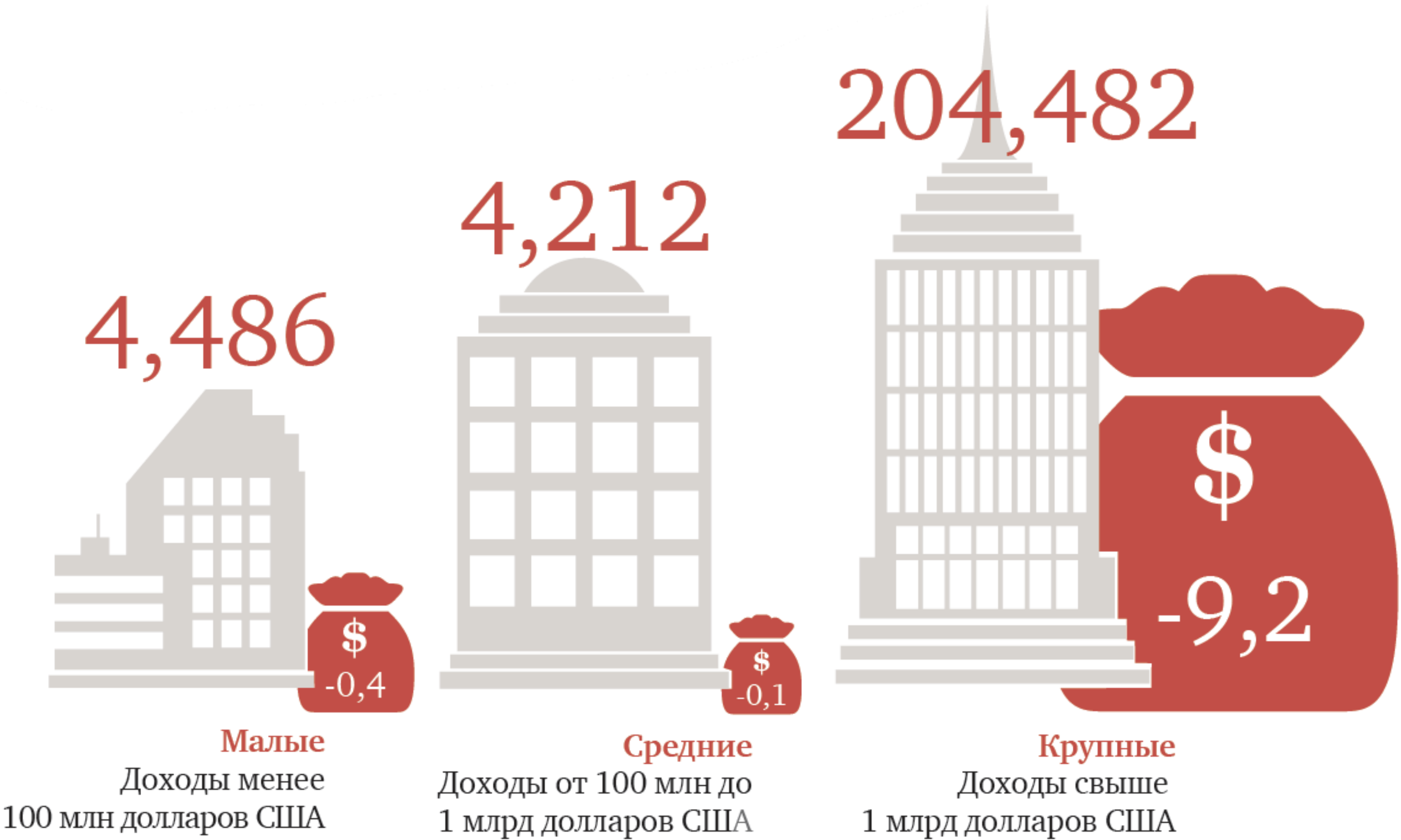


PWC

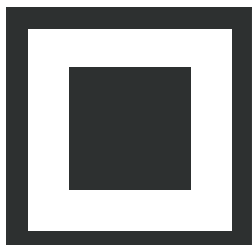


КОЛИЧЕСТВО ИНЦИДЕНТОВ ИБ И УЩЕРБ (\$ МЛН.)

по России, 2014

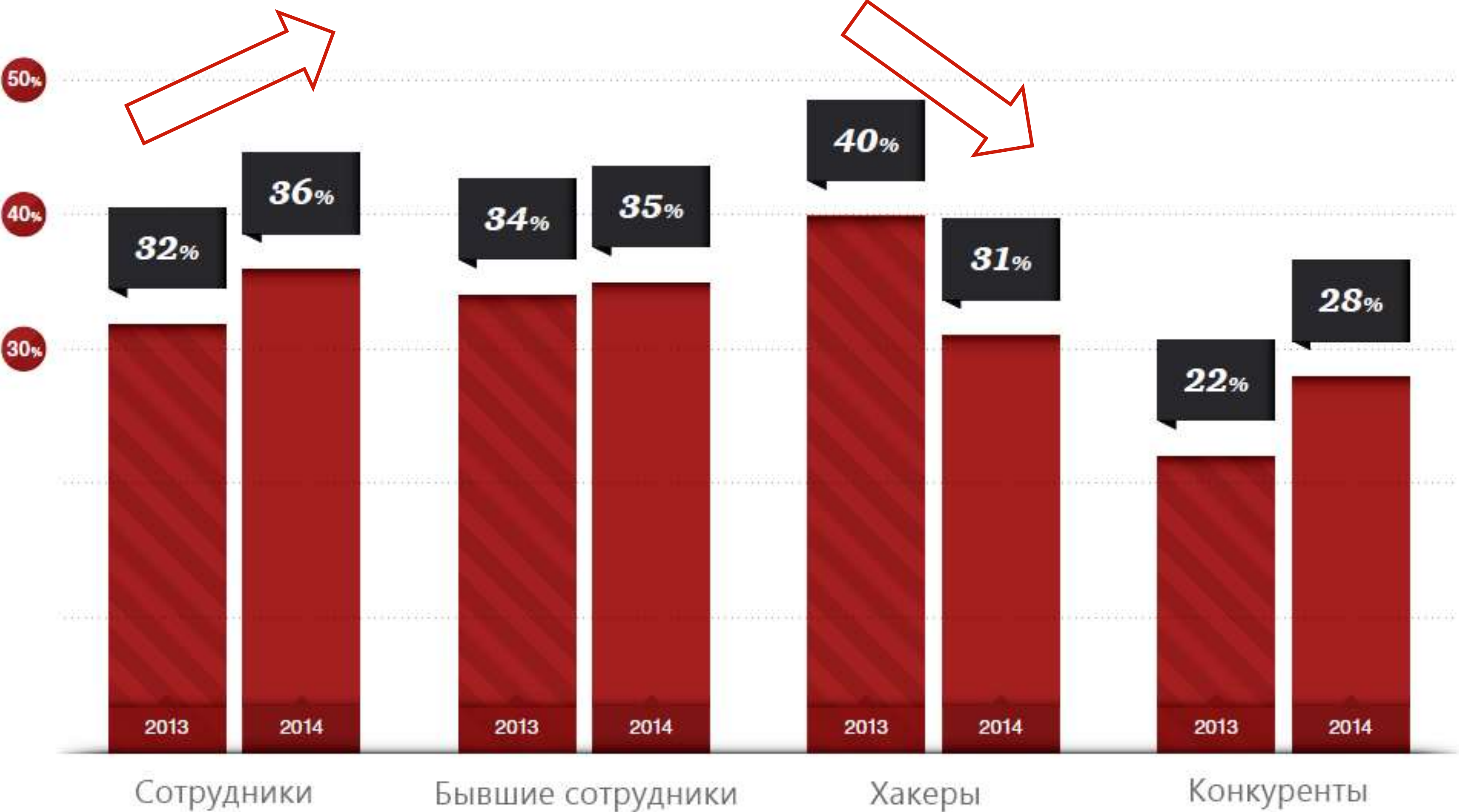


PWC



ИЗМЕНЕНИЕ ДОЛИ ИСТОЧНИКОВ ИНЦИДЕНТОВ ИБ

2013-2014



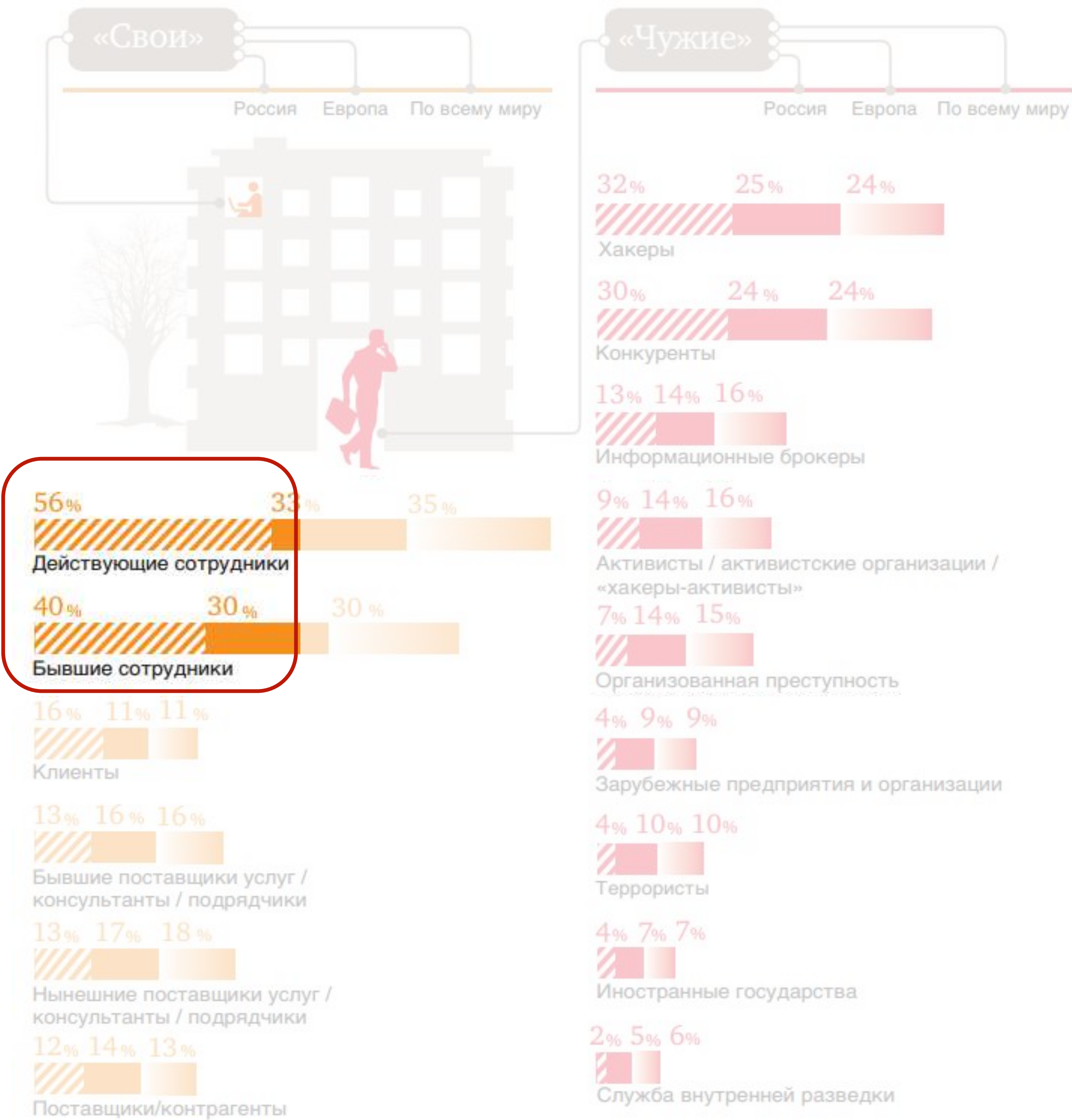
PWC

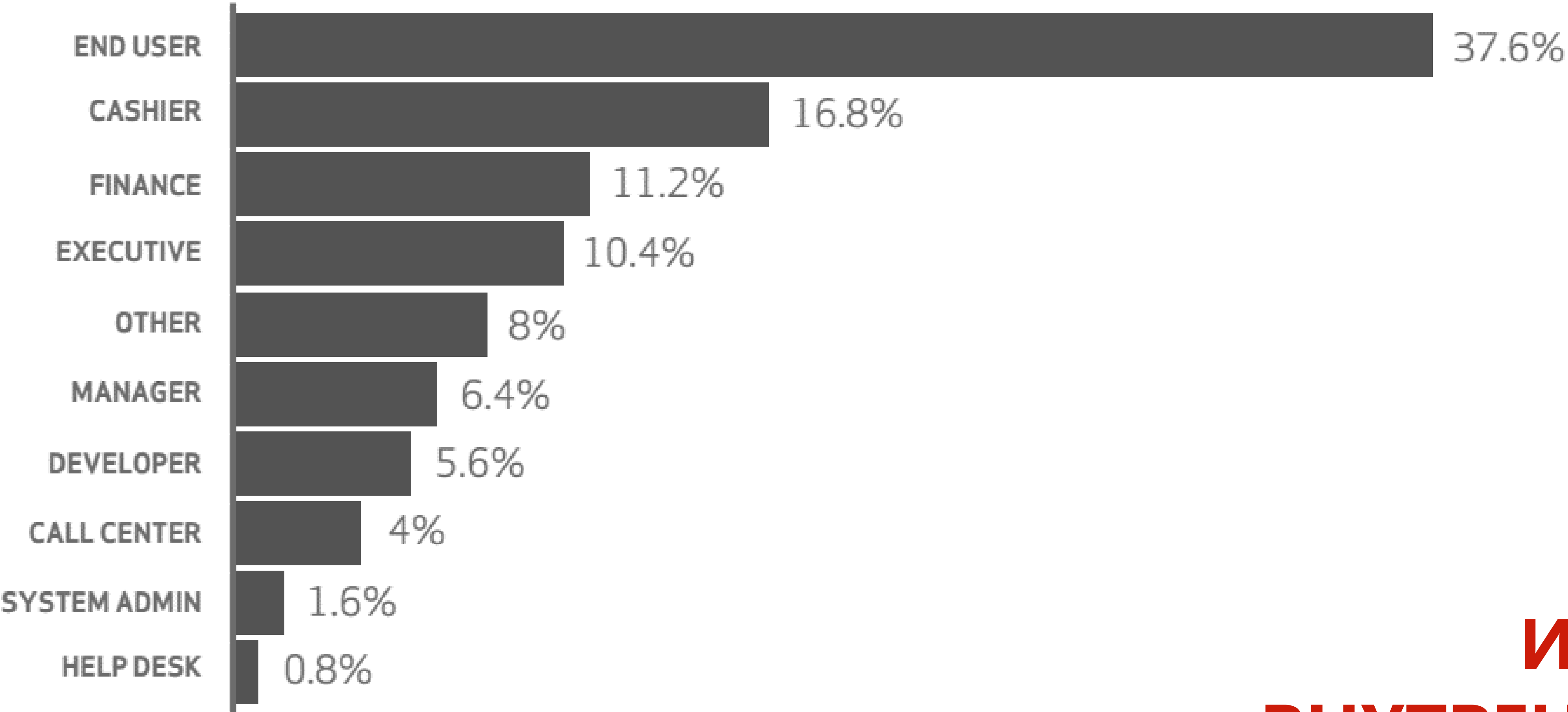
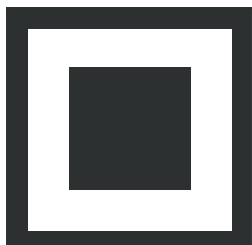
ВИНОВНИКИ

ИНЦИДЕНТОВ ИБ

«СВОИ» или «ЧУЖИЕ»

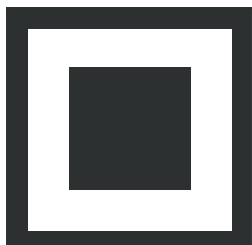
2013-2014





ИСТОЧНИКИ ВНУТРЕННИХ УГРОЗ

Verizon



ИСТОЧНИКИ ВНУТРЕННИХ УГРОЗ

JSOC

ПРИЧИНЫ И СЛЕДСТВИЯ КИБЕРПРЕСТУПЛЕНИЙ СОТРУДНИКОВ



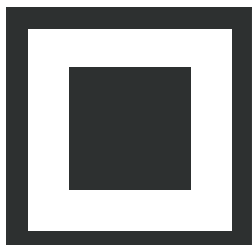
НАИБОЛЕЕ ЗНАЧИМЫЕ УЯЗВИМОСТИ С ТОЧКИ ЗРЕНИЯ РИСКОВ ИБ

2014



Приоритет: 1 2 3 4 5

EY



ПРАВА ДОСТУПА СОТРУДНИКОВ – СЛАБОЕ МЕСТО 2/3 ОРГАНИЗАЦИЙ

PWC

...

Сотрудники являются угрозой для кибербезопасности,
а управление доступом является слабым местом

...

Ручное управление доступом и редкий аудит позволяют легко
получить избыточный доступ к данным

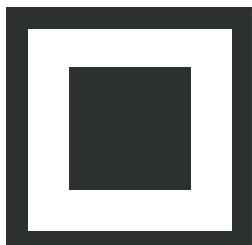
...

Ключевые зоны риска – новые сотрудники, бывшие
сотрудники, и смена подразделений

...

ПОКА ОРГАНИЗАЦИИ ИЩУТ ХАКЕРОВ, КОТОРЫЕ ПРОНИКАЮТ
ИЗВНЕ, МОШЕННИЧЕСТВО ПРОИСХОДИТ ИЗНУТРИ

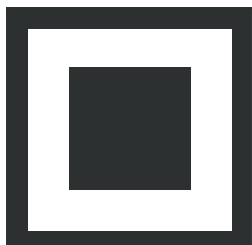




АВТОМАТИЗАЦИЯ КОНТРОЛЯ ДОСТУПА СОТРУДНИКОВ СОКРАЩАЕТ РИСКИ ИБ



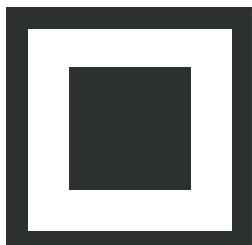
*IdM – Identity Management, класс систем управления правами доступа сотрудников



КАК РАБОТАЕТ IDM?



Ситуация	Автоматизация в IdM
Сотрудника приняли на работу	IdM выдал базовые права
Изменились данные сотрудника	IdM обновил данные в системах
Сотрудник запросил доступ через IdM, ответственные согласовали доступ через IdM	IdM назначил права по заявке, отозвал по истечении срока действия
Сотрудник сменил должность	IdM создал заявку на пересмотр прав
Сотрудника уволили	IdM отозвал все права доступа
Сотруднику назначили права в обход IdM	IdM оповестил/исправил
Сотрудник забыл пароль УЗ	Оператор сменил пароль УЗ сотрудника
Скомпрометированы УЗ сотрудника	Офицер ИБ заблокировал все УЗ сотрудника
Требуется провести аудит доступа сотрудников	Выдана информация о правах доступа: -кто/куда имеет доступ -кто и когда его запросил/согласовал -какие права были в прошлом ...и многое другое



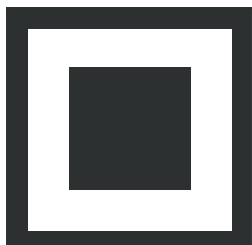
БИЗНЕС-ЭФФЕКТ ОТ ВНЕДРЕНИЯ IDM

- ❖ Снижение на **20% РИСКОВ** нарушений информационной безопасности
- ❖ Экономия **50% ВРЕМЕНИ** бизнес-пользователей на решение проблем через службу технической поддержки
- ❖ Экономия времени персонала на проведение процесса периодического пересмотра прав доступа – **8 ЧАСОВ В ГОД ДЛЯ КАЖДОГО ЗАДЕЙСТВОВАННОГО СОТРУДНИКА**

Forrester Research

- ❖ Сокращение времени сбора данных для расследований **50%**
- ❖ Ожидание доступа новыми сотрудниками сокращается **С 3-4 ДНЕЙ ДО 2-4 ЧАСОВ**
- ❖ Экономия времени ИТ-персонала – **14%**

IDC



КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

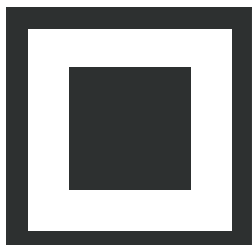
НАШ БЭКГРАУНД

- ❖ Несколько десятков проектов
- ❖ На 7 различных решениях
- ❖ С доработками до 70%

#CODEIB

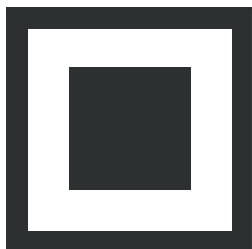


Г. НОВОСИБИРСК
10 СЕНТЯБРЯ 2015



ЧТО МЫ ПОЛОЖИЛИ
В ОСНОВУ НАШЕГО IDM?



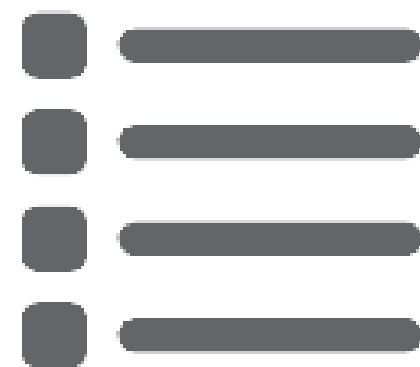


ОСОБЕННОСТИ INRIGHTS



ИНТЕРФЕЙС

-разработан профессионалами в области Usability



МНОГОЗАДАЧНОСТЬ

-Управление УЗ,
-группами,
-ролями и т.д.



РАСШИРЯЕМОСТЬ

-Расширение схемы
-Добавление объектов
-Скриптовые языки



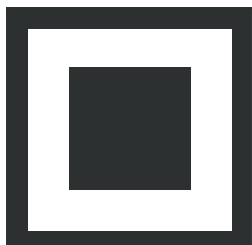
ЦЕЛОСТНОСТЬ

-Управление изменениями
-Контроль ошибок
-Защита УЗ



ПОДДЕРЖКА СТАНДАРТОВ И ИНСТРУМЕНТОВ

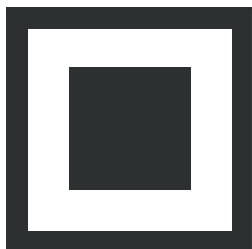
-REST API, SOAP, WSDL
-Jasper Reports
-BPMN



ЧЕМ INRIGHTS ХОРОШ ДЛЯ ВАС?

- ❖ Красивый и удобный пользовательский интерфейс
 - ❖ Интерфейс разработан одной из лучших компаний в области Usability по заказу Solar Security и учитывает особенности требований пользователей IdM крупнейших российских организаций
- ❖ Сравнительно небольшой срок внедрения
 - ❖ Учитывает «подводные камни» внедрения IdM и требования крупнейших российских компаний
 - ❖ Настраивается под нестандартные требования там, где это необходимо
 - ❖ Мастер установки и преднастроенные шаблоны конфигурации
- ❖ Обновляемый без потери доработок
 - ❖ Доработки расширяют функционал и отделяются от штатного кода
 - ❖ Механизм обновления не затирает доработки

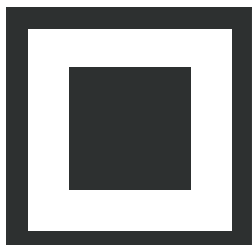




ПОЛЕЗНЫЕ ОТЧЕТЫ ПО ИБ

1. JSOC Security flash report Q1 2015
2. ISACA, State of Cybersecurity: Implications for 2015. An ISACA and RSA Conference Survey
3. PwC. Управление киберрисками во взаимосвязанном мире. Основные результаты Глобального исследования по вопросам обеспечения информационной безопасности. Перспективы на 2015 год
4. Get ahead of cybercrime. EY's Global Information Security Survey 2014
5. Verizon 2015 Data Breach Investigations Report





КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

СПАСИБО ЗА ВНИМАНИЕ!
ВОПРОСЫ?



ДМИТРИЙ БОНДАРЬ

РУКОВОДИТЕЛЬ
НАПРАВЛЕНИЯ INRIGHTS,
SOLAR SECURITY

КОНТАКТЫ

ТЕЛ. +7 (499) 755-07-07
d.bondar@solarsecurity.ru

#CODEIB



Г. НОВОСИБИРСК
10 СЕНТЯБРЯ 2015