

Актуальные проблемы привилегированного доступа к IT-системам и **SafeInspect** как ВОЗМОЖНОЕ решение

Проблема → Задача → Решение

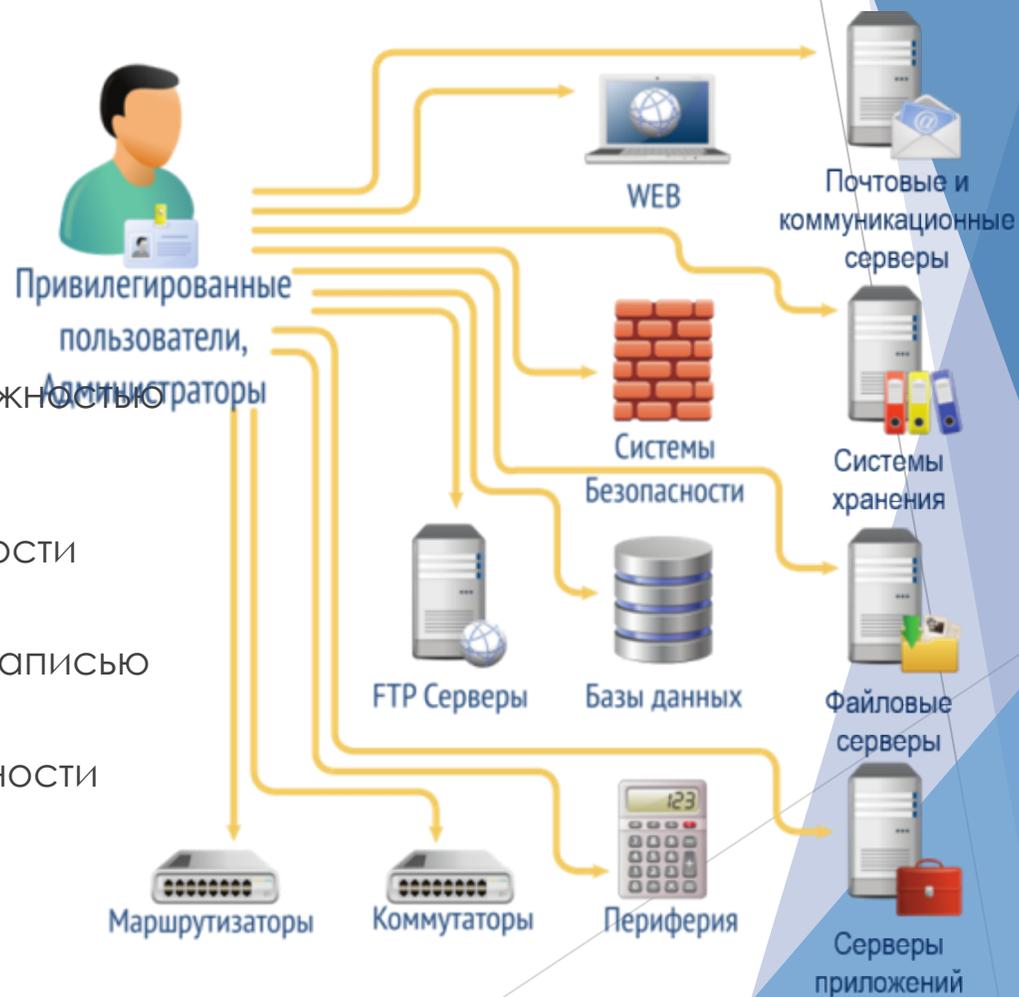
ООО НТБ 2017

Наша история



Привилегированный пользователь. Кто он?

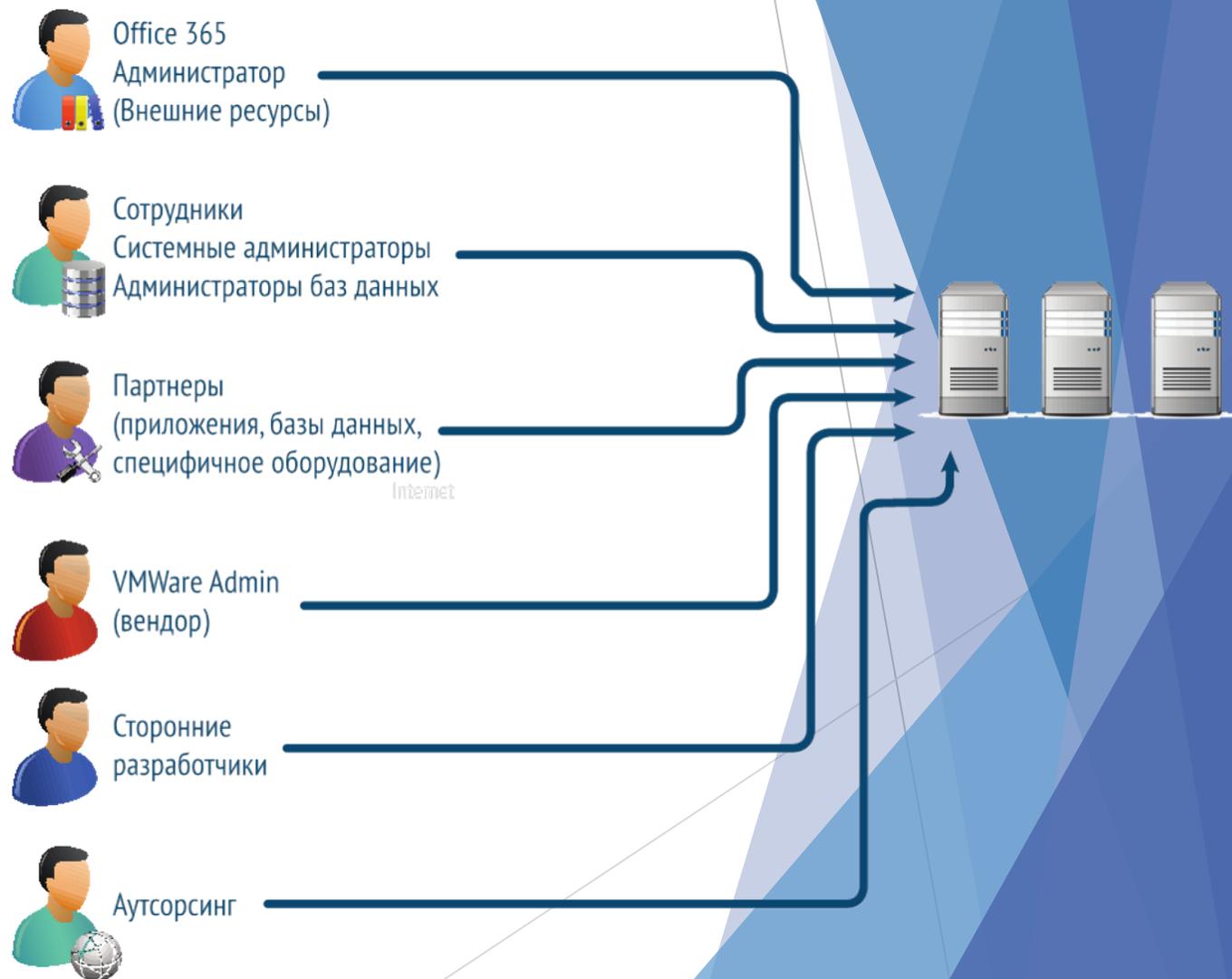
- ▶ Есть в каждой организации
- ▶ Внутренний сотрудник или сотрудник компании-подрядчика
- ▶ В достаточной степени квалифицированный
- ▶ Имеет полный доступ ко всей IT-системе с возможностью удалять/изменять любые данные и изменять конфигурацию оборудования
- ▶ Зачастую имеет доступ к критичным для деятельности организации системам и данным
- ▶ Зачастую производит работы под одной учетной записью с коллегами
- ▶ Имеет возможность удалять следы своей деятельности
- ▶ Бывает обидчив :)



Всем ли можно доверять? Риски

- ▶ Внутренние сотрудники, если их 2-3 могут быть доверенными. А десять?
- ▶ Подрядчики, вендоры:
 - компетентны?
 - добросовестны?
 - получают доступ только туда куда нужно?
 - соблюдают SLA?

Какой ущерб вы понесете из-за отказа IT-системы?



Ущерб

- ▶ Бывший администратор *Allegro MicroSystems LLC* используя служебный ноутбук подключился к корпоративной сети и добавил в модуль *Oracle* код, уничтожающий ценные данные

ущерб – \$100 000

- ▶ Администратор неназванного банка в Нигерии сотрудничал с хакерами и помог установить соединение с базой данных банка и совершить кражу средств

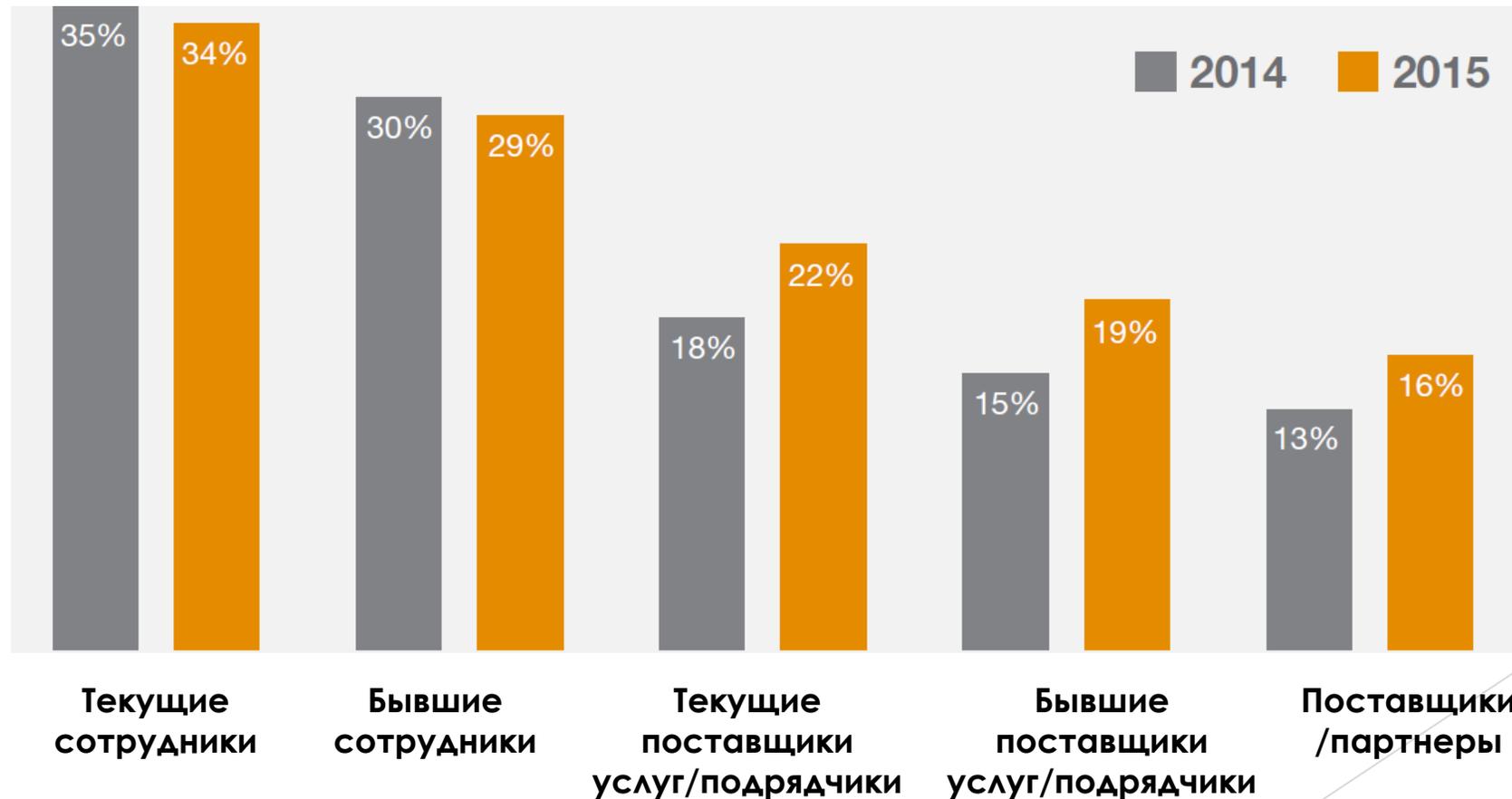
ущерб – \$38,6 млн

- ▶ Подрядчик *Tata Consultancies* похитил документацию *Epic Systems*, составляющую коммерческую тайну

ущерб – \$240 млн

Исследование PricewaterhouseCoopers 2016 год

Виновники инцидентов информационной безопасности



Требования нормативных документов

- ▶ Приказ № 17, 21 и 31 ФСТЭК России
- ▶ Приказ № 135 Минкомсвязи России (п.8)
- ▶ Стандарт Банка России по обеспечению информационной безопасности организаций банковской системы Российской Федерации (СТО БР ИББС)
- ▶ Payment Card Industry Data Security Standard (PCI DSS) 3.2 (Requirement 2, 7, 8 и 10)

Проблема: Доступ обслуживающего персонала к критически важной инфраструктуре никак не контролируется

Задача: Обеспечить контроль

Решение:  **Safelnspect**

Принцип работы Safelnspect –

отслеживание управляющего

трафика от

привилегированного

пользователя к

информационным системам



SafeInspect позволяет:

КОНТРОЛИРОВАТЬ



Все действия привилегированных сотрудников будут записаны в недоступное для них хранилище

УПРАВЛЯТЬ ДОСТУПОМ



Полный доступ только к необходимым IT-системам и на определенный регламентом срок.

ОПЕРАТИВНО РАССЛЕДОВАТЬ



В случае инцидентов информационной безопасности можно быстро установить виновника и масштабы проблемы.

УСИЛИТЬ ЗАЩИТУ ИНФРАСТРУКТУРЫ



Возможна интеграция с уже имеющимися решениями по обеспечению ИБ, что усилит защиту инфраструктуры.

Цели внедрения

- ▶ Контроль подрядчиков/аутсорсеров
- ▶ Контроль вендоров оборудования
- ▶ Контроль получения администраторских прав
- ▶ Дополнительная защита доступа к критически важным частям IT-системы
- ▶ Контроль соблюдения SLA
- ▶ Защита своих интересов аутсорсерами
- ▶ Легитимизация удаленного доступа для персонала
- ▶ Дополнительный сервис в «облаках»

Преимущества SafeInspect

- ▶ Не зависит от используемых платформ
- ▶ Наблюдение в реальном времени
- ▶ Может быть «незаметным» для контролируемого лица
- ▶ Простое внедрение и использование
- ▶ Минимальное влияние на бизнес-процессы
- ▶ Интеграция с другими средствами обеспечения ИБ
- ▶ Оптимальная политика ценообразования
- ▶ Российская разработка (№3341 в реестре ПО)
- ▶ Гибкий подход к решению самых разных задач ИБ
- ▶ Ваша уверенность в безопасности IT-инфраструктуры

Благодарю за внимание!

Александр Трофимов

Директор по работе с ключевыми клиентами
ООО «Новые технологии безопасности»

тел. моб.: 8-9999-8-7777-8

тел./факс: (499) 647-48-72

atrofimov@newinfosec.ru