ДиалогНаука

Стандарт PCI DSS

Александр Крупчик

CISA, CISM, CISSP, PCI QSA, PCI ASV

ДиалогНаука

Информация о PCI DSS

- **Выпущен:** 30 июня 2005 года
- **Разработку инициировали:** MasterCard Worldwide, Visa International, American Express, Discover Financial Services, JCB
- **Цель:** Обеспечить защиту электронных платежных систем в свете участившихся случаев хищений информации о держателях платежных карт
- **Обязателен для внедрения:** Во всех организациях, хранящих, обрабатывающих и передающих данные о держателях платежных карт: процессинговые компании, банки, Интернет-магазины и др.
- **Развитие:** Актуальная версия стандарта 2.0, ввод в действие 3.0 (до конца 2014)

ДиалогНаука

Кому необходим PCI DSS

Требования стандарта PCI DSS распространяется на организации, обрабатывающие, хранящие или передающие информацию о держателях платежных карт, например:

- Процессинговые компании
- Банки, имеющие собственный процессинг
- Крупные розничные сети
- Операторы сотовой связи
- Интернет-магазины
- Коммерческие ЦОД

ДиалогНаука

Терминология PCI DSS

Merchat (Торгово-сервисное предприятие)

- Принимают платежные карты для оплаты товаров или услуг (розничные сети, рестораны, Интернет-магазины и т.д.)

Сервис-провайдер (Поставщик услуг)

- Оказывают различные услуги, необходимые для осуществления оплаты (банки, процессинги и т.д.)

Транзакция

- Операция с картой по оплате, снятию или переводу денежных средств

QSA (Qualified Security Assessor)

- Компания имеющая право проводить аудиты по PCI DSS

ASV (Approved Scanning Vendor)

- Компания, имеющая право проводить внешние сканирования уязвимостей

ДиалогНаука

Процедуры подтверждения соответствия сервис-провайдеров

Уровни сервис-провайдеров

- Level 1 > 300 тыс. транзакций в год
- Level 2 < 300 тыс. транзакций в год

Процедуры подтверждения соответствия

- Ежегодный сертификационный аудит, выполняемый QSA (Level 1)
- Ежегодное заполнение самоопросника Self-Assessment (Level 2)
- Ежеквартальное внешнее сканирование уязвимостей, проводимое ASV (Level 1, 2)
- Ежеквартальное внутреннее сканирование уязвимостей (Level 1, 2)
- Ежегодное выполнение внутренних и внешних тестов на проникновение (Level 1, 2)
- Ежегодное выполнение анализа рисков (Level 1, 2)

ДиалогНаука

Последствия несоответствия

- Ущерб от действий злоумышленников (финансовый и репутационный)
- Отказ в повышении статуса в платежных системах
- Штрафные санкции (размеры штрафов конфиденциальны)
- Отказ международных платежных систем в предоставлении услуг

ДиалогНаука

Состав услуг PCI DSS

- Услуги по сертификации включают три этапа:
  - Обследование ИС заказчика и разработка рекомендаций по приведению в соответствие
  - Реализация требований стандарта
  - Сертификация

ДиалогНаука

Состав услуг PCI DSS

- Обследование ИС заказчика и разработка рекомендаций по приведению в соответствие
  - Обследование
  - Разработка плана мероприятий по приведению в соответствие

ДиалогНаука

Состав услуг по PCI DSS

- Реализация требований стандарта
  - Разработка политик, стандартов и процедур
  - Проектирование СОИБ
  - Внедрение СОИБ

ДиалогНаука

Состав услуг PCI DSS

- Услуги по сертификации
  - Анализ рисков ИБ
  - Ежеквартальные ASV-сканирования
  - Ежеквартальные сканирования уязвимостей из ЛВС
  - Тестирование на проникновение из сети Интернет и ЛВС
  - Сертификационный аудит

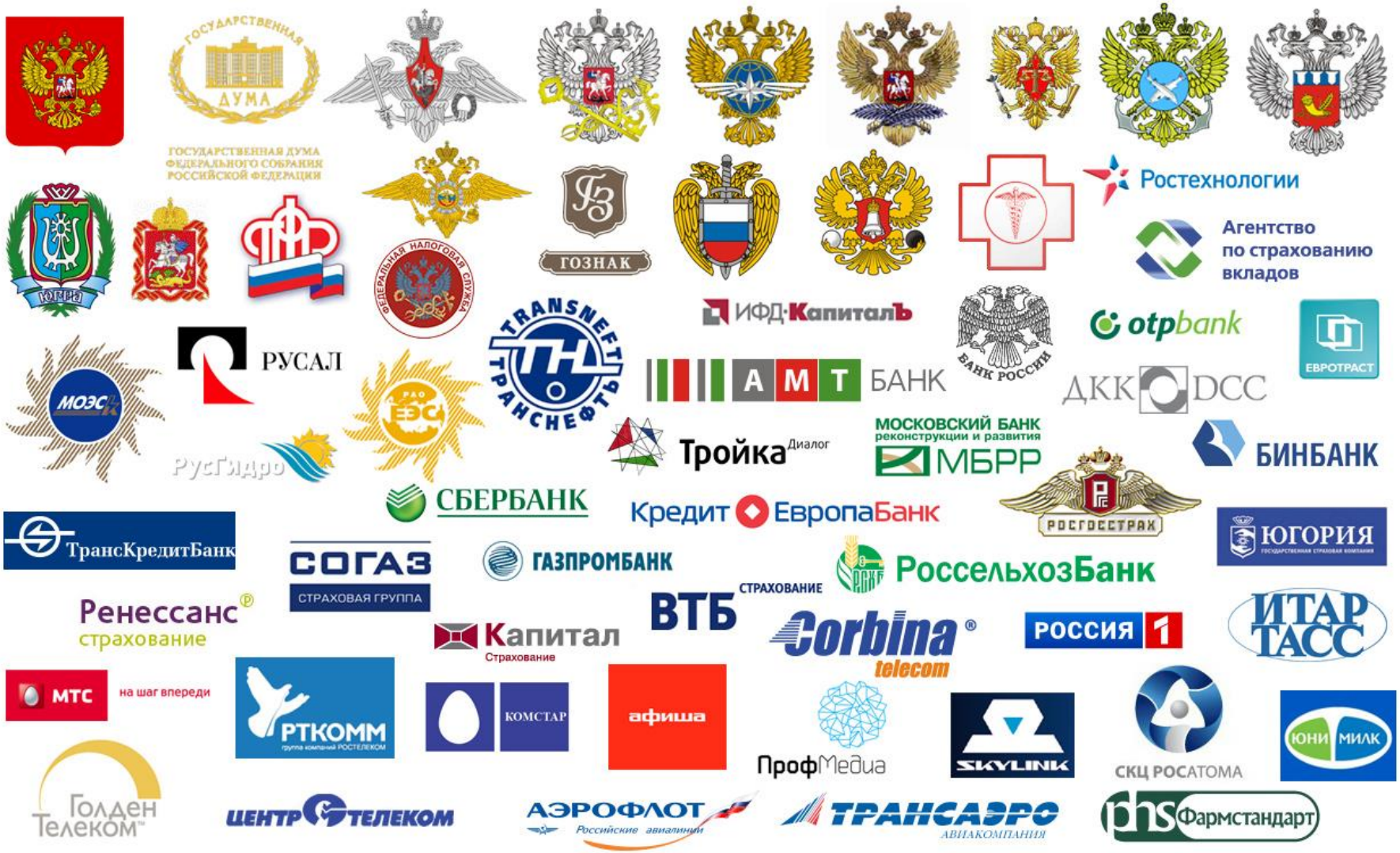
ДиалогНаука

Наши преимущества

- Необходимые компетенции
- Большой опыт выполнения работ (7 лет) по внедрению PCI DSS и проведению сертификации по PCI DSS
- Гибкость при приведении в соответствие и сертификации
- Возможность выполнения комплексных проектов вместе с НПС и СТО БР

ДиалОгНаука

О компании «ДиалогНаука»: ключевые клиенты



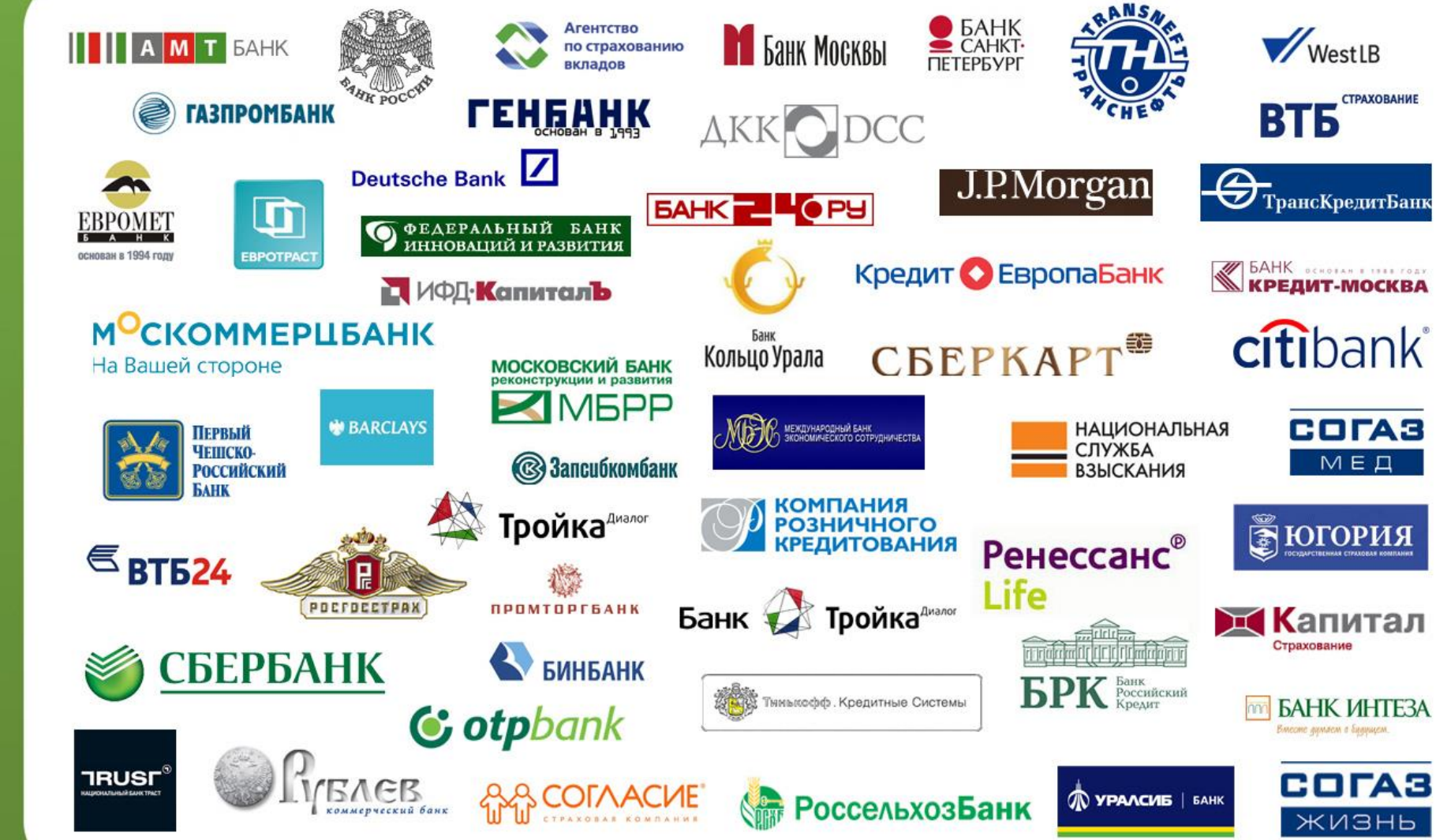
ДиалогНаука

О компании «ДиалогНаука»: клиенты кредитно-финансового и страхового сектора

Банк России
ТрансКредитБанк
Сбербанк
РоссельхозБанк
Кредит Европа Банк
Тройка Диалог
Газпромбанк
Московский банк реконструкции и развития МБРР
Deutsche Bank
АМТ Банк
Запсибкомбанк
ИФД Капиталъ
otpbank
Национальная служба взыскания
ДКК DCC
Бинбанк
Банк 24.ру
Тинькофф. Кредитные Системы
Евротраст
Transneft Транснефть
ВТБ Страхование
СОГАЗ Страховая группа
Ренессанс страхование
Капитал Страхование
Росгосстрах
Югория
Согласие

ДиалОгНаука

О компании «ДиалогНаука»: клиенты кредитно-финансового и страхового сектора



Ваши вопросы?

Александр Крупчик
Тел.: +7 (495) 980-67-76,164
Факс: +7 (495) 980-67-75
Моб.: +7 (916) 147-08-20
E-mail: krupchik@dialognauka.ru

ЗАО «ДиалогНаука»
http://www.DialogNauka.ru