Уральский Центр Систем Безопасности

Технологии защиты бизнеса.
Аудит. Проектирование.
Внедрение. Сопровождение.

Выполнение требований PCI DSS для систем торгового эквайринга. Практический опыт

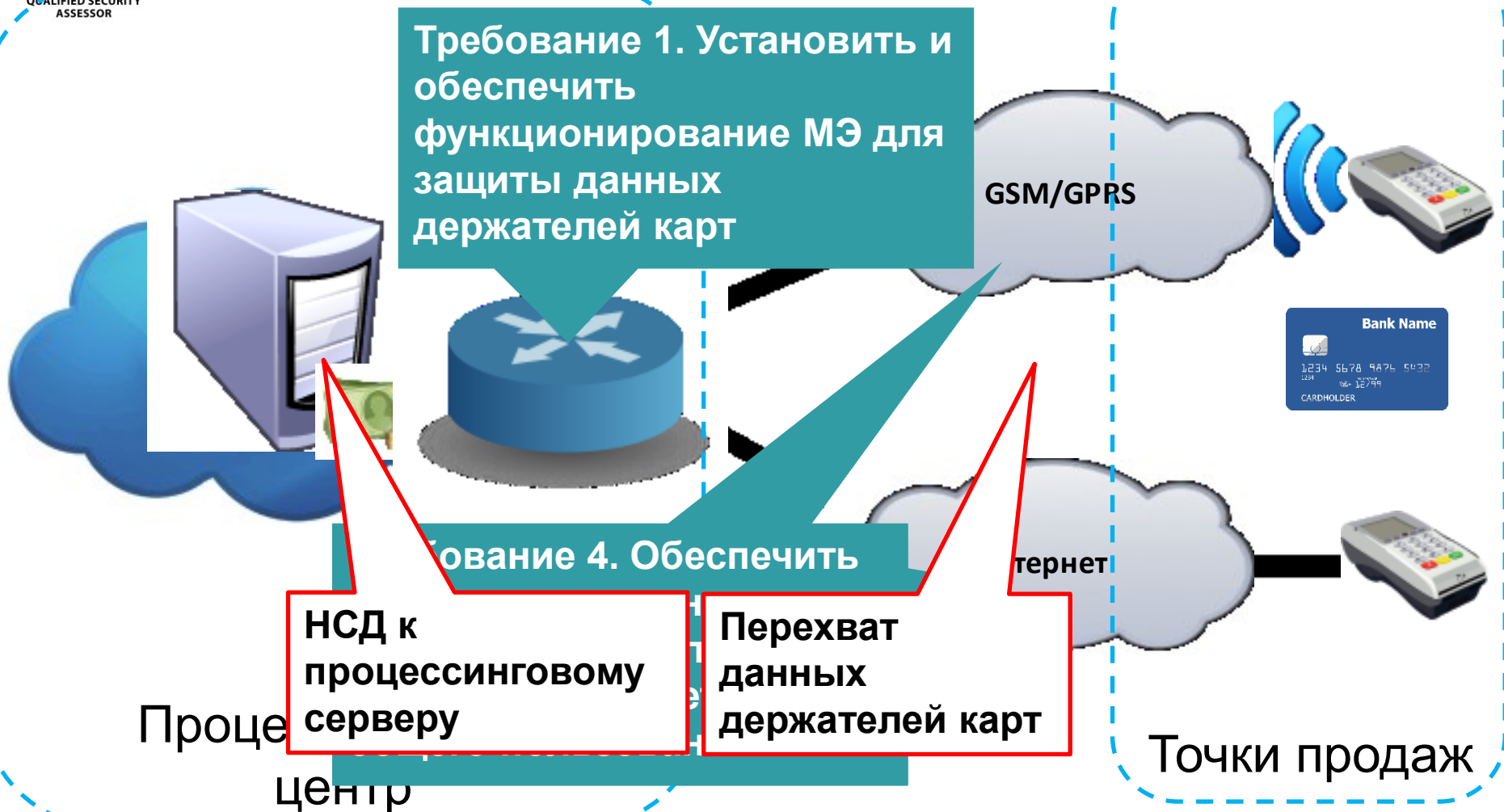
Домуховский Николай

главный инженер Департамента Системной Интеграции

02.06.2014

PCI Security Standards Council
QUALIFIED SECURITY ASSESSOR

Система торгового эквайринга



Требования к системе защиты данных торгового эквайринга

PCI Security Standards Council
QUALIFIED SECURITY ASSESSOR

Требования по защите данных держателей карт

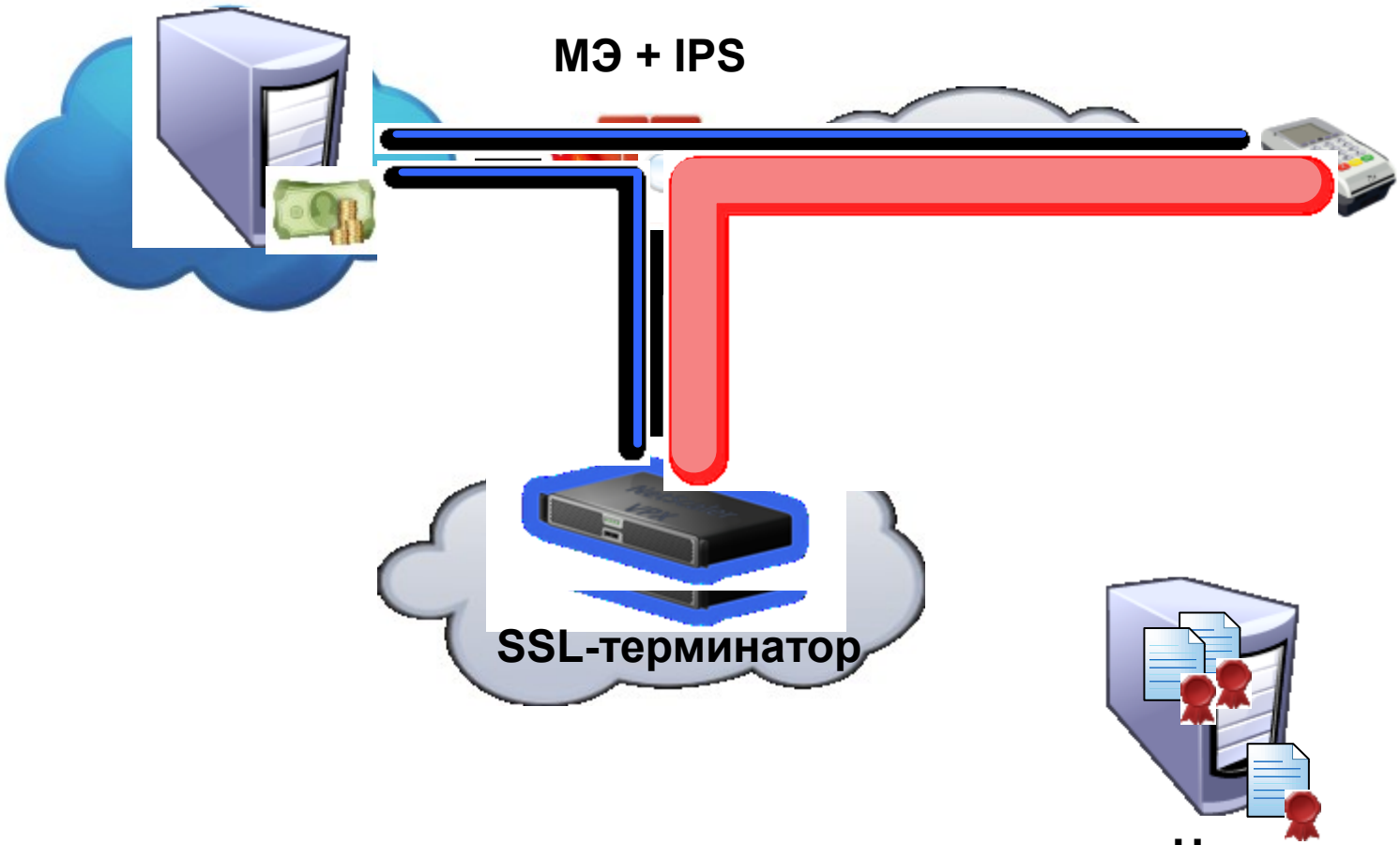
- Защита периметра (Требование 1)
- Шифрование данных держателей карт (Требование 4)
- Обнаружение и предотвращение вторжений (Требование 11.4)
- Управление криптографическими ключами (Требования 3.5, 3.6)

Выбор решения по защите данных держателей карт

Вариант решения	Плюсы	Минусы
Граница сегмента ПЦ: UTM **Точки продаж:** VPN-шлюзы	• Решение не зависит от возможностей ПО процессингового центра и PoS-терминалов	• сильные ограничения по масштабированию • высокая стоимость (как начальная, так и каждого последующего подключения)
Граница сегмента ПЦ: МЭ+IPS **Точки продаж:** –	• Высокая масштабируемость • Низкая стоимость подключения • Отсутствует необходимость установки доп. оборудования со стороны торговых точек	• Необходима доработка ПО процессинга и/или PoS-терминала • Высокая начальная стоимость

PCI Security Standards Council
QUALIFIED SECURITY ASSESSOR

Система защиты данных торгового эквайринга



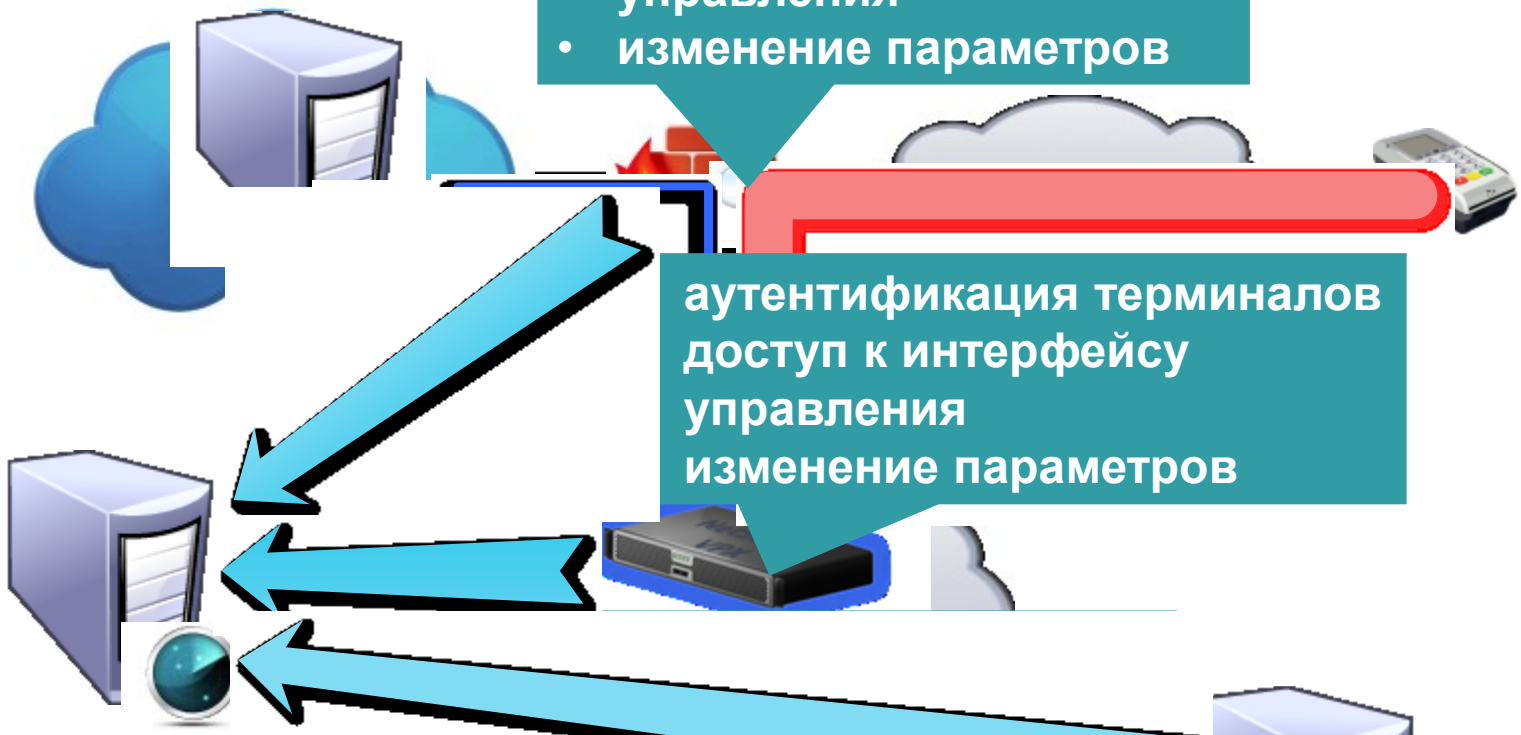
Уральский Центр Систем Безопасности

Технологии защиты бизнеса.
Аудит. Проектирование.
Внедрение. Сопровождение.

QUALIFIED SECURITY ASSESSOR

Система защ ого эквайринга. Сб ий ИБ

- сетевой доступ в сегмент ПЦ
- сетевые атаки
- доступ к интерфейсу управления
- изменение параметров



аутентификация терминалов
доступ к интерфейсу управления
изменение параметров

Средство сбора и анализа событий ИБ

изменение параметров

Актуальность использования средства анализа и корреляции событий ИБ

- Дополнительная защита журналов событий от несанкционированной модификации
- Автоматическое выявление инцидентов ИБ: блокировки учетных записей, ошибки аутентификации PoS-терминалов и пр.
- Автоматизация требований PCI DSS по анализу журналов событий
- Средства анализа и корреляции событий ИБ, как правило, есть у Заказчика до начала проекта

QUALIFIED SECURITY ASSESSOR

Управление доступом к системным компонентам

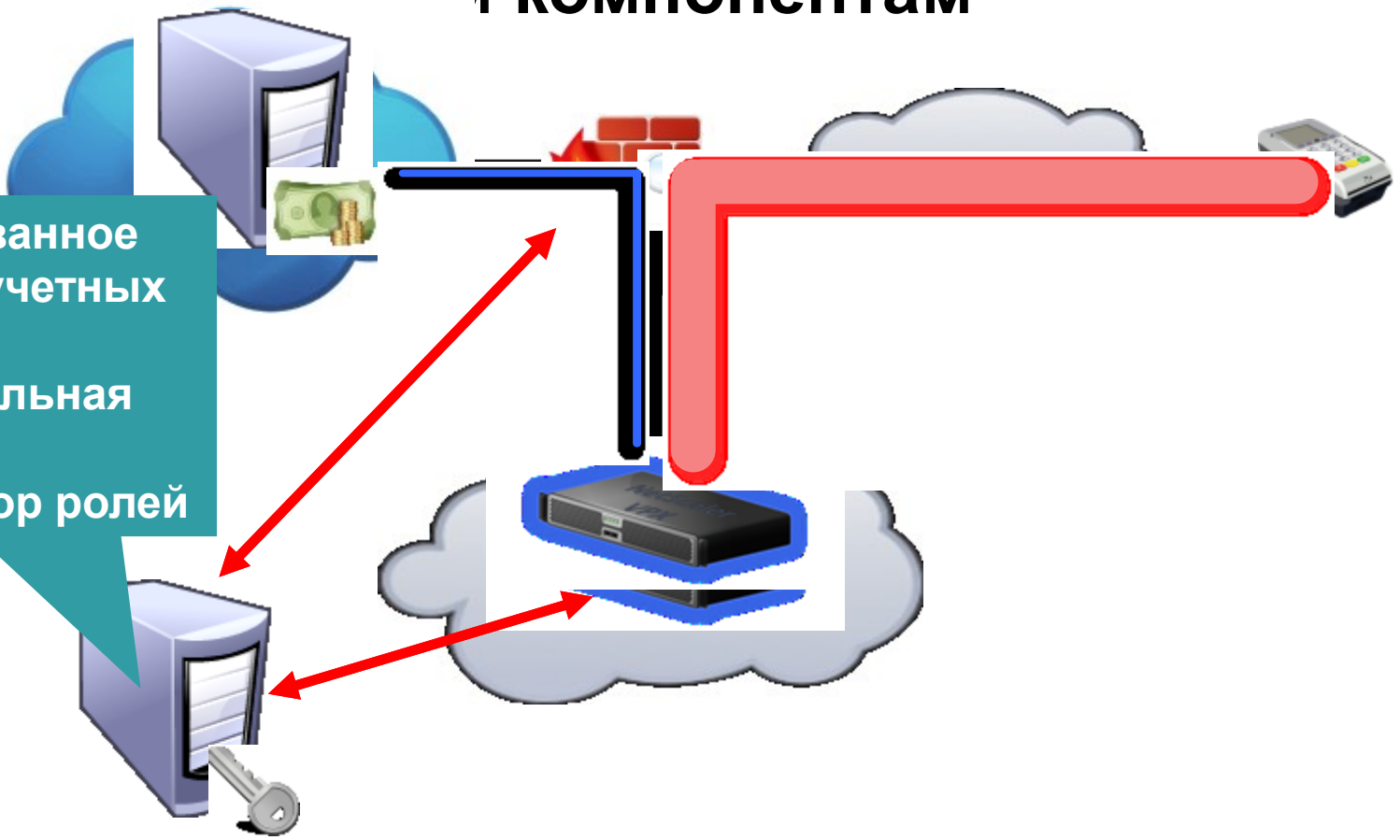
Системный компонент	Роль	Доступные операции
Межсетевой экран	Администратор	Все
	Администратор безопасности	Просмотр событий Редактирование ACL
IPS	Администратор	Все
	Администратор безопасности	Просмотр событий Редактирование политики
	Оператор	Просмотр событий
SSL-терминатор	Администратор	Все, кроме управления криптографическими ключами
	Администратор безопасности	Просмотр событий Управление криптографическими ключами

Итого: 3 группы устройств, 7 ролей, учетных записей - ?

PCI Security Standards Council
QUALIFIED SECURITY ASSESSOR

Система защиты данных торгового эквайринга. Управление доступом к системным компонентам

- Централизованное хранилище учетных записей
- Единая парольная политика
- Единый набор ролей



AAA сервер

PCI Security Standards Council
QUALIFIED SECURITY ASSESSOR

Обеспечение надежности

Обеспечение надежности

PCI Security Standards Council
QUALIFIED SECURITY ASSESSOR

Высокая доступность решения

- Применение отказоустойчивых конфигураций
- Использование «байпас» режимов
- Формирование комплектов ЗИП

Диагностика

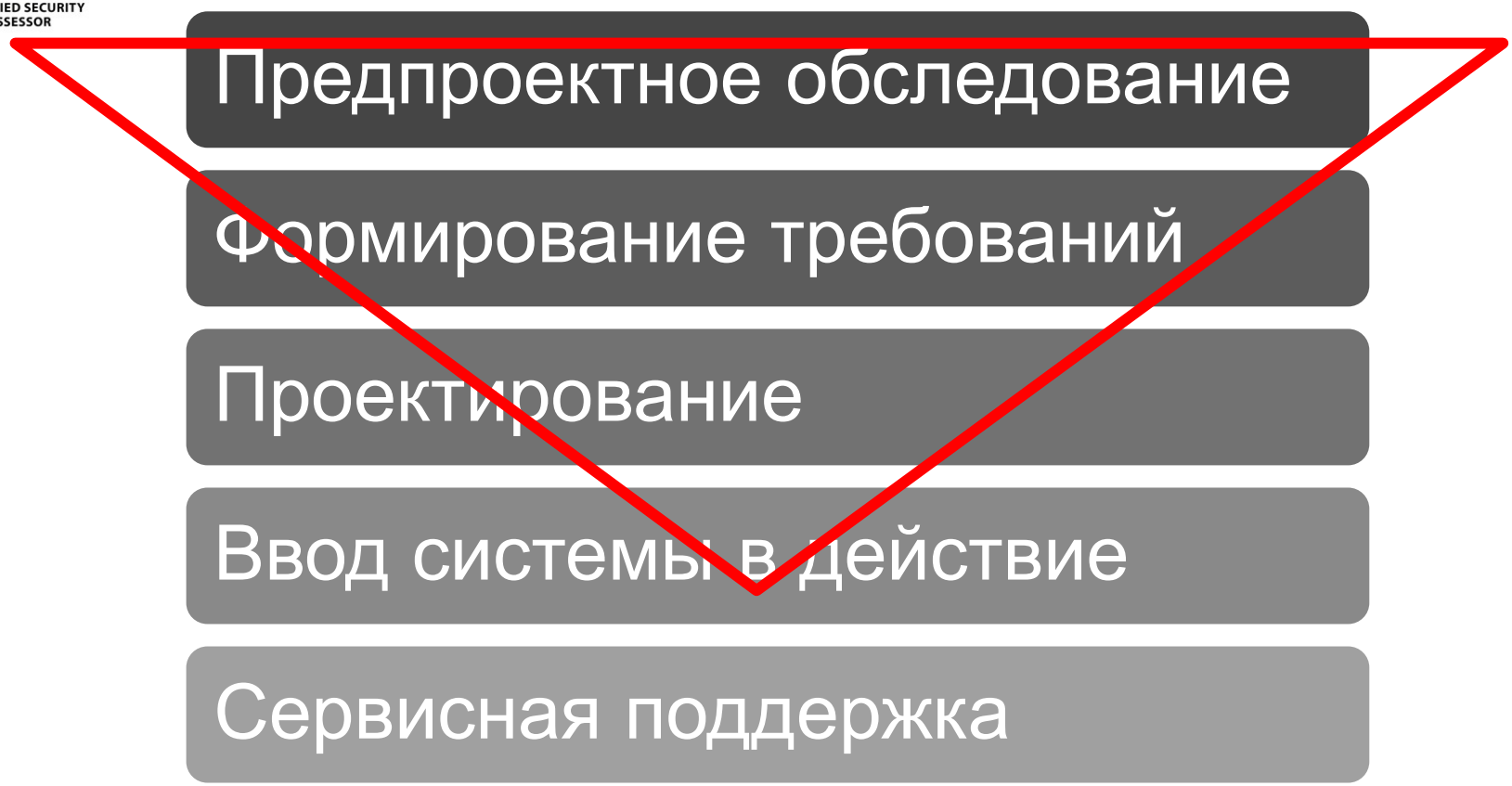
- Диагностика работоспособности оборудования
- Мониторинг нагрузки на оборудование
- Предупреждение отказов

Подготовка персонала

- Инструкции по поиску и устранению неисправностей
- Отработка аварийных ситуаций

QUALIFIED SECURITY ASSESSOR

Подход ООО «УЦСБ». Стадии проекта



PCI Security Standards Council
QUALIFIED SECURITY ASSESSOR

Предпроектное обследование. Проблемы и решения

Основное подразделение Заказчика не располагает данными

- **Взаимодействие со смежными подразделениями Заказчика**
- **Анализ внутренней документации Заказчика с целью определения зон ответственности**

Запрашиваемые данные не могут быть предоставлены

- **Заключение СоК**
- **Сбор исключительно необходимых данных**

Данные отсутствуют

- **Применение инструментальных средств сбора данных**
- **Выход на разработчика (например, системы торгового эквайринга)**

PCI Security Standards Council
QUALIFIED SECURITY ASSESSOR

Формирование требований. Полнота охвата

Проектирование. Комплексный подход

PCI Security Standards Council
QUALIFIED SECURITY ASSESSOR

PCI Security Standards Council
QUALIFIED SECURITY ASSESSOR

Ввод в действие. Планирование и контроль

Планирование работ по вводу в действие

- Привлечение специалистов Заказчика (подразделения по ИБ, удостоверяющий центр, службы эксплуатации ИТ инфраструктуры)
- Выявление критичных работ и необходимых технологических окон
- Оценка рисков для сервиса и подготовка планов восстановления

Выполнение работ

- Фиксация результатов
- Контроль успешности выполнения каждой задачи
- Оперативное изменение основного плана (реагирование на риски)

Контроль результатов

- Разработка программы и методики испытаний
- Период опытной эксплуатации
- Ведение журнала опытной эксплуатации

QUALIFIED SECURITY ASSESSOR

Благодарю за внимание!
Вопросы?

Домуховский Николай

ООО «УЦСБ»
620026, Екатеринбург, ул. Ткачей, д. 6
Тел.: +7 (343) 379-98-34
Факс: +7 (343) 229-57-38
info@ussc.ru
www.USSC.ru