НТЦ ВУЛКАН

Реализация проектов по созданию комплексной системы защиты объектов КИИ от категорирования до проверки ФСТЭК: Взгляд интегратора

Алексей Орехов

Руководитель производственно-технологического управления

www.ntc-vulkan.ru

НТЦ «ВУЛКАН» - НЕЗАВИСИМЫЙ ЭКСПЕРТ И ИНТЕГРАТОР ТЕХНОЛОГИЙ ИБ

На рынке с **2010** года

150+ сотрудников в штате

Комплексные решения в сфере экономической и информационный безопасности

Сертифицированная система менеджмента качества

500+ реализованных проектов в ИБ

Входит в **40** крупнейших компаний РФ в сфере защиты информации

По версии TAdviser, 2022

20+ проектов внедрения SIEM

Допуски и лицензии ФСТЭК, ФСБ, Минобороны, Минпромторг

НТЦ ВУЛКАН

НАШ ОПЫТ ОСНОВАН НА ВЗАИМОДЕЙСТВИИ БОЛЕЕ ЧЕМ С 200 ОРГАНИЗАЦИЯМИ

Финансовый сектор: кредитные и некредитные финансовые организации

СБЕР
Тинькофф Банк
БАНК РОССИЯ
БАНК САНКТ-ПЕТЕРБУРГ
МТС БАНК
СНГБ
СБЕР СТРАХОВАНИЕ
Тинькофф Страхование
ДОМ РФ
ИНФИНИТУМ
СОГАЗ СТРАХОВАЯ ГРУППА
ИНГОССТРАХ
Спасибо
МОСКОВСКАЯ БИРЖА
НАЦИОНАЛЬНЫЙ РАСЧЕТНЫЙ ДЕПОЗИТАРИЙ
НАЦИОНАЛЬНЫЙ КЛИРИНГОВЫЙ ЦЕНТР
QIWI
БКС

Телекоммуникации и связь

Ростелеком
МегаФон
МТС
Билайн
TELE2
МТТ

Государственные структуры и организации

АИС Налог-3
ДИТ
Информационный город
ТУРИЗМ.РФ

ТЭК и производственные предприятия

ЛУКОЙЛ Нефтяная компания
РусГидро
Мосэнерго
РОС РАО
Роскосмос
СУХОЙ

Прочие компании широкого спектра отраслей

СВЯЗНОЙ
B2B CENTER
ОТС.RU Группа электронных площадок
СИБИНТЕК
nexters
МИКРОХЕМ

НТЦ ВУЛКАН

ОБЩАЯ ПРОБЛЕМАТИКА «НА ВХОДЕ»

- Построенная бессистемно, «по наитию», непрозрачная и недокументированная инфраструктура, где годами наслаивались решения разных производителей
- Проприетарность ПО АСУ ТП и монополизм производителей ведут к незаинтересованности в изменениях
- Продолжительность жизненного цикла систем (прежде всего АСУ ТП) превышает продолжительность цикла обновления нормативных требований
- Большой временной лаг между завершением проектных работ и началом внедрения
- «Осложнения», связанные со слияниями, поглощениями и формированием сложных структур владения
- Отсутствие единой мотивации и несовпадение «целей» для подразделений эксплуатирующих АСУ ТП и подразделений ИБ

Обеспечение безопасности ЗОКИИ

- ✓ Прозрачность инфраструктуры
- ✓ Ревизия присвоенных категорий
- ✓ Анализ критических процессов
- ✓ Авторитетные рекомендации

НТЦ ВУЛКАН

КАНОНИЧЕСКИЙ ПОДХОД К СОЗДАНИЮ СИСТЕМЫ

Этап 1 — **Предпроектное обследование**

Этап 2 — **Разработка проектной документации**

Этап 3 — **Разработка организационно-распорядительной документации**

Этап 4 — **Поставка, установка и настройка СрЗИ**

Этап 5 — **Внедрение мер по защите информации, в т.ч. организационных**

Этап 6 — **Проведение испытаний / Оценка соответствия / Оценка эффективности**

НТЦ ВУЛКАН

КОМПЛЕКСНОЕ ОБСЛЕДОВАНИЕ

НТЦ ВУЛКАН

ИСХОДНЫЕ ДАННЫЕ ДЛЯ ПРОЕКТИРОВАНИЯ

Состав ИС	Субъекты доступа ИС	Внешние связи ИС	Обработка информации	Структура и функции	Функции СПО и ППО	Персонал
• Тип оборудования • Назначение • Операционная система • Прикладное программное обеспечении • Наличие технической поддержки	• Сотрудники субъекта • Не сотрудники субъекта • Внешние информационные системы • Цели доступа • …	• Способы доступа • Интерфейсы доступа • Сетевые порты и протоколы • Используемые линии связи • …	• Способы получения информации • Способы передачи информации • Цели информационного обмена • …	• Используемые технологии • Распределенность • …	• Обеспечение процессов • Взаимодействие • ...	• Организационно-штатная структура • Численность • Квалификация • …

+ ПРОЦЕССЫ

Более 150 метрик !

НТЦ ВУЛКАН

ПОДХОДЫ К ПРОЕКТИРОВАНИЮ

НТЦ ВУЛКАН

ВНЕДРЕНИЕ – ТЕХНИЧЕСКИЕ СРЕДСТВА

Встроенные средства

- Настройка
- Наличие техподдержки

Наложенные средства

- Закупка\Поставка
- Развертывание в инфраструктуре
- Настройка
- Оценка влияния на технологические процессы

НТЦ ВУЛКАН

ВНЕДРЕНИЕ – ПРОЦЕССЫ

Ограничения программной среды

Идентификация и аутентификация

Защита ИС и ее компонентов

Управление доступом

Информирование и обучения персонала

Настройка и ввод в эксплуатацию

Антивирусная защита

Обеспечение действий в нештатных ситуациях

Управление конфигурацией

Планирование мероприятий по обеспечению защиты информации

Реагирование на компьютерные инциденты

Совершенствование

Эксплуатация

Управление обновлениями ПО

Аудит безопасности

Предотвращение вторжений

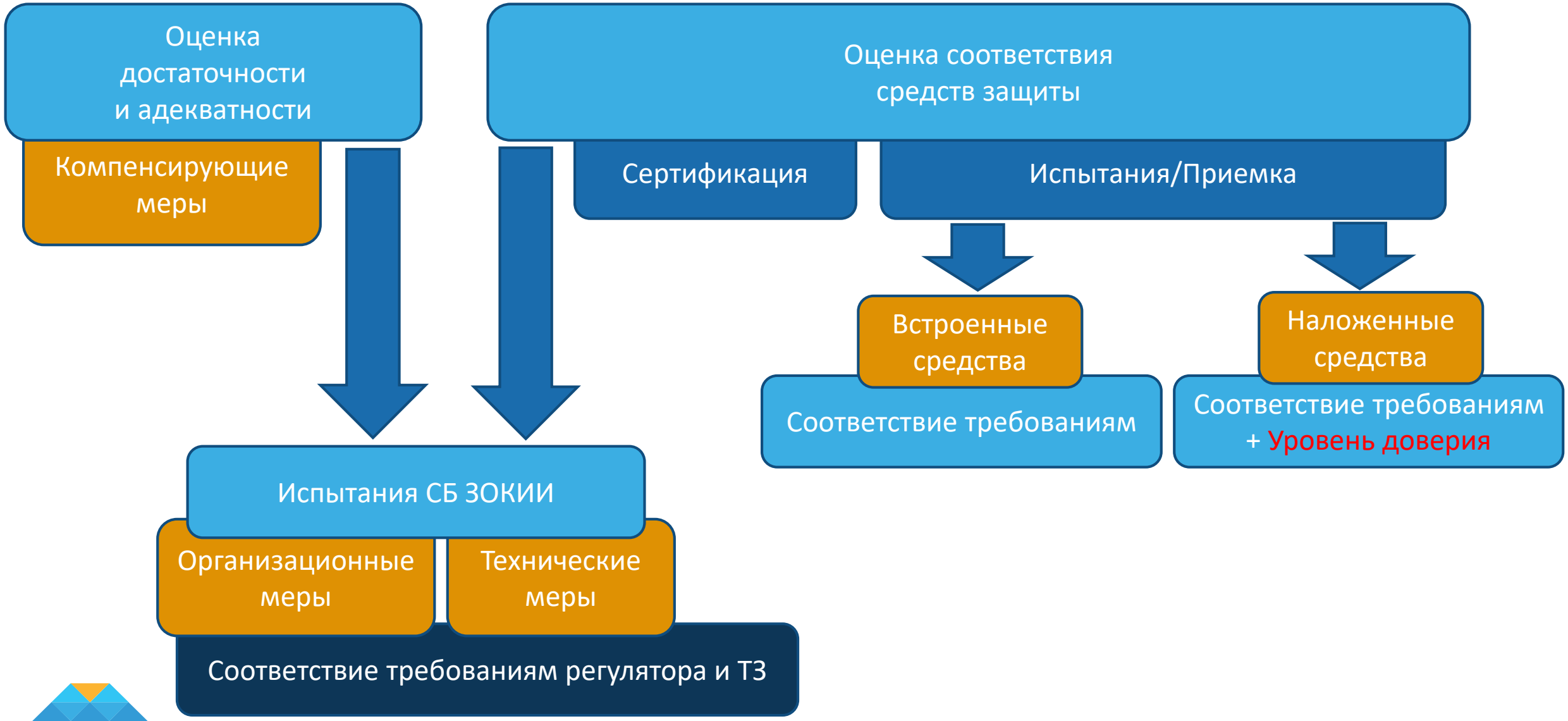
Защита машинных носителей информации

Взаимодействие служб ИТ, АСУ и ИБ !!!

Защита технических средств и систем

НТЦ ВУЛКАН

ВВОД В ЭКСПЛУАТАЦИЮ



НТЦ ВУЛКАН

ПРОВЕРКА РЕГУЛЯТОРА

Технические средства	Процессы	ОРД и проектная документация
• Настройка • Достаточность	• Соответствие ОРД • Достаточность • «Следы»	• Соответствие реальной системе • Соответствие требованиям регулятора
Качество проектирования	**Обучение персонала**	**Качество обследования**

НТЦ ВУЛКАН

РЕЗУЛЬТАТ - КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ЗОКИИ

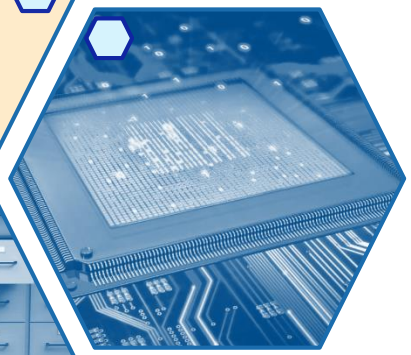
Реализация процессов
Обеспечение безотказной
повседневной работы

Соответствие
изменяющимся нормам
Возможность противостоять
новым компьютерным атакам

1. Эксплуатация

2. Контроль

3. Изменения



4. Обучение

Актуализация
и контроль знаний
персонала для эксплуатации
модернизированной системы

Модернизация
всех\отдельных
составляющих с целью обеспечения
возможности нейтрализации актуальных
компьютерных атак

НТЦ ВУЛКАН

СПАСИБО ЗА ВНИМАНИЕ!

НТЦ ВУЛКАН

Научно-технический центр «Вулкан»
г. Москва, ул. Ибрагимова, д. 31
+7 495 777-13-10
marketing@ntc-vulkan.ru

www.ntc-vulkan.ru