НТЦ ВУЛКАН

«Программные, технические и организационные решения системы управления информационной безопасностью на предприятиях энергетической отрасли»

Орехов Алексей Юрьевич

Руководитель проектно-технологического управления

25.04.2024

www.ntc-vulkan.ru

КРИТИЧЕСКАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА (КИИ)

Обобщение опыта реализации проектов в следующих отраслях

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

Правительство Российской Федерации

Президент Российской Федерации

Федеральная служба безопасности Российской Федерации

Минцифры России

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации

Федеральная служба по техническому и экспортному контролю Российской Федерации

МИНИСТЕРСТВО ЭНЕРГЕТИКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

НТЦ ВУЛКАН

Систематизация проблемных аспектов

ОБЯЗАННОСТИ СУБЪЕКТА КИИ

НТЦ ВУЛКАН

КАТЕГОРИИ ЗНАЧИМОСТИ КИИ

Категорирование ОКИИ - установление соответствия ОКИИ критериям значимости и показателям их значений, присвоение ему одной из категорий значимости, проверка сведений о результатах ее присвоения

Присвоение ОКИИ категории значимости
либо
принятие решения об отсутствии необходимости присвоения ОКИИ одной из категорий значимости

Определение социальной значимости	Определение политической значимости	Определение экономической значимости	Определение экологической значимости	Определение значимости для обороны страны, безопасности государства и правопорядка
оценка возможного ущерба, причиняемого жизни или здоровью людей, возможности прекращения или нарушения функционирования объектов обеспечения жизнедеятельности населения, транспортной инфраструктуры, сетей связи, а также максимальном времени отсутствия доступа к государственной услуге для получателей такой услуги	оценка возможного причинения ущерба интересам Российской Федерации в вопросах внутренней и внешней политики;	оценка возможного причинения прямого и косвенного ущерба субъектам критической информационной инфраструктуры и (или) бюджетам Российской Федерации	оценка уровня воздействия на окружающую среду	

Предусмотрено 3 категории значимости

Систематизация проблемных аспектов

ГЕТЕРОГЕННАЯ СРЕДА АСУ ТП

Проприетарность ПО АСУ ТП и монополизм производителей ведут к незаинтересованности в изменениях

Продолжительность жизненного цикла систем АСУ ТП превышает продолжительность цикла обновления нормативных требований

Конфликт интересов между вендром АСУ ТП и ИТ (инфраструктура)

Конфликт интересов между вендором АСУ ТП и ИБ (СУИБ)

Поддержка АСУ ТП фрагментарная и вне общих планов мероприятий

➔ **Нужно выстраивать взаимодействие!**

➔ **Вендору нельзя давать «угонять» систему!**

ПРОЦЕССЫ ОБЕСПЕЧЕНИЯ ИБ НА БУМАГЕ И ФАКТИЧЕСКИ

Процессы	По документам	Фактически
Антивирусная защита	АВ закуплены и установлены, ежегодно приобретается поддержка	Базы данных АВ на АСУ ТП не обновлялись с момента установки
Обеспечение действий в нештатных ситуациях	Написаны и лежат в папках инструкции для персонала	Ни один из сотрудников не может ответить на вопрос, что он будет делать
Идентификация и аутентификация	Приказом регламентированы «сложные» пароли	qwe123, 12345678 …
Защита машинных носителей информации	Существуют журналы доверенных носителей	В USB портах рабочих станций заряжают телефоны

и многое другое...

ТОЧКА ОТСЧЕТА

Построенная «по наитию», слабо документированная инфраструктура, где годами наслаивались решения разных производителей

Продолжительность жизненного цикла систем (прежде всего АСУ ТП) превышает продолжительность цикла обновления нормативных требований

Проприетарность ПО АСУ ТП и монополизм производителей ведут к незаинтересованности в изменениях

Отсутствие единой мотивации и несовпадение «целей» для подразделений эксплуатирующих АСУ ТП и подразделений ИБ

Большой временной лаг между завершением проектных работ и началом внедрения

«Осложнения», связанные со слияниями, поглощениями и формированием сложных структур владения

Указ Президента РФ от 30 марта 2022 года № 166 «О мерах по обеспечению технологической независимости и безопасности КИИ»

Организации, ведущие закупки по 223-ФЗ:

с 31.03.2022 не могут закупать иностранное ПО, в т.ч. В составе ПАК и СрЗИ тоже

с 2025 года нельзя использовать иностранное ПО (и ПАК, и СрЗИ) на своих значимых ОКИИ

Постановление Правительства Российской Федерации от 14.11.2023 г. № 1912 «О порядке перехода субъектов КИИ на преимущественное применение доверенных программно-аппаратных комплексов на принадлежащих им ЗОКИИ»

с 1 сентября 2024 г. не допускается использование ПАК, приобретенных с 1 сентября 2024 г. и не являющихся доверенными программно-аппаратными комплексами

До 1 января 2030 года переход 100%

ФОРМАЛЬНЫЙ ПОДХОД - ПРОЕКТИРОВАНИЕ

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

Результаты и проблемы формального подхода

ФОРМАЛЬНЫЙ ПОДХОД - ВНЕДРЕНИЕ

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

ВЫЯВЛЯЕМЫЕ ПРОБЛЕМЫ

- Неверное определение границ ЗОКИИ
- Отсутствие контроля сетевого трафика
- Отсутствие сегментации сети
- Использование открытых протоколов передачи
- «Плоские» права доступа в ЗОКИИ
- Отсутствие управления идентификаторами/аутентификаторами
- Отсутствие контроля интерфейсов ввода-вывода
- Осуществляются не все процессы обеспечения информационной безопасности
- Неполные процессы обеспечения информационной безопасности

На разных этапах жизненного цикла

- ✓ Категорирование
- ✓ Проектирование
- ✓ Внедрение
- ✓ Эксплуатация

НЕВЕРНОЕ ОПРЕДЕЛЕНИЕ ГРАНИЦ ЗОКИИ

Состав ИС | **Субъекты доступа ИС** | **Внешние связи ИС** | **Обработка информации** | **Функции СПО и ППО** | **Персонал**

«Распиливание» ППО на модули

- Отсутствие необходимых механизмов защиты
- Необходимость контроля соединений между модулями
- Множество взаимодействующих/обеспечивающих ИС

Широкие границы объекта

- Большие затраты на создание системы защиты
- Отсутствие средств защиты для некоторых компонент
- «Зоопарк» технических средств

Узкие границы объекта

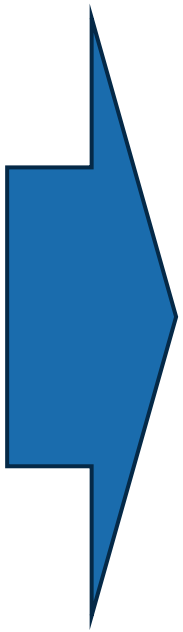
- Появление множества взаимодействующих ИС
- «Разрыв» технологического (критического) процесса

- ✓ Программные и аппаратные компоненты, осуществляющие критический процесс
- ✓ Средства защиты информации
- ✓ Инфраструктурные компоненты

«ПЛОСКИЕ» ПРАВА ДОСТУПА В ЗОКИИ

Состав ИС | **Субъекты доступа ИС** | Внешние связи ИС | Обработка информации | Функции СПО и ППО | Персонал

- Отсутствие разграничение прав между администраторами
- Пользователи с одинаковыми правами
- Пользователи с правами администраторов



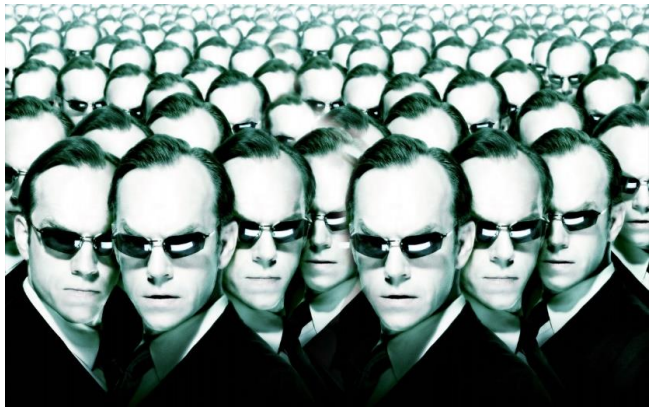
- ✓ Разграничение прав доступа встроенными механизмами
- ✓ «Терминирование» доступа
- ✓ Использование PAM-систем

ОТСУТСТВИЕ УПРАВЛЕНИЯ ИДЕНТИФИКАТОРАМИ/АУТЕНТИФИКАТОРАМИ

Состав ИС | **Субъекты доступа ИС** | Внешние связи ИС | Обработка информации | Функции СПО и ППО | Персонал

Top 20 паролей

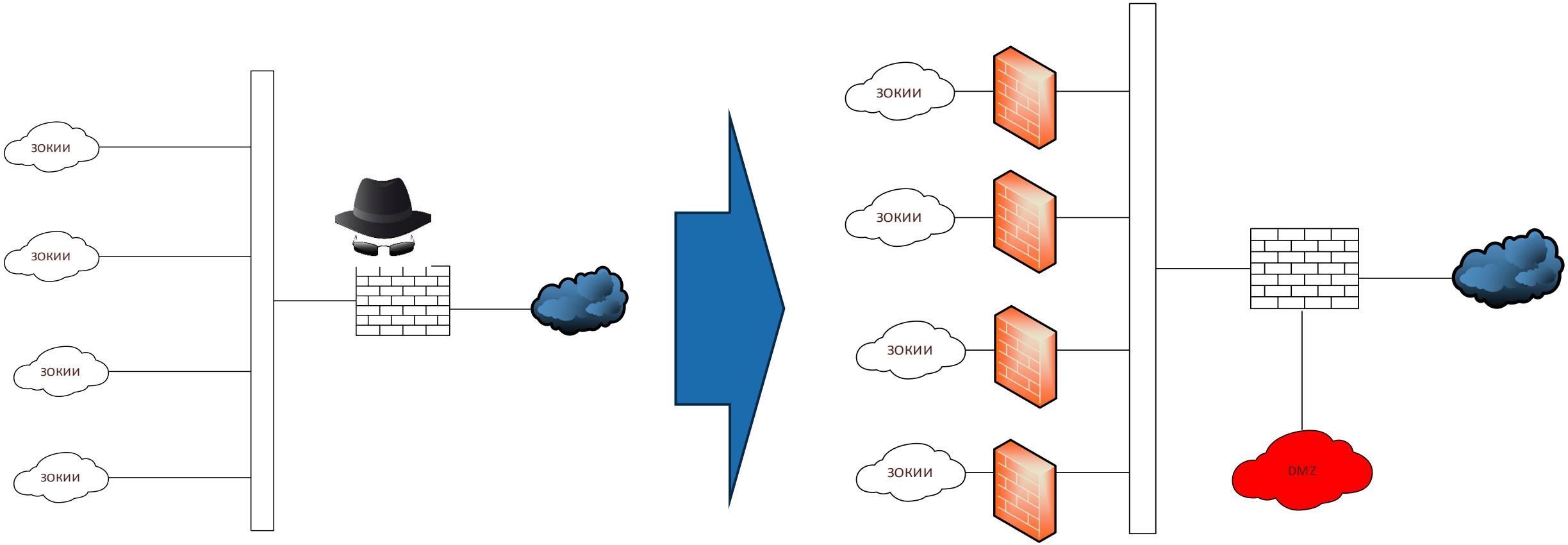
Gmail	Yandex	Mail.ru
123456	123456	qwerty
password	123456789	123456
123456789	111111	qwertyuiop
qwerty	qwerty	qwe123
12345678	1234567890	qweqwe
111111	1234567	klaster
abc123	7777777	1qaz2wsx
123123	123321	1q2w3e4r
1234567	000000	qazwsx
1234567890	123123	1q2w3e
iloveyou	666666	123qwe
password1	12345678	1q2w3e4r5t
000000	555555	123456789
zaq12wsx	654321	111111
tinkle	gfhjkm	zxcvbnm
qwerty123	777777	1234qwer
monkey	112233	qwer1234
target123	121212	asdfgh
dragon	987654321	marina
1q2w3e4r	159753	q1w2e3r4t5



- ✓ Управление формированием идентификатора
- ✓ Управление сложностью аутентификатора
- ✓ Управление сменой аутентификатора
- ✓ Блокирование учетных записей (в том числе по неактивности)

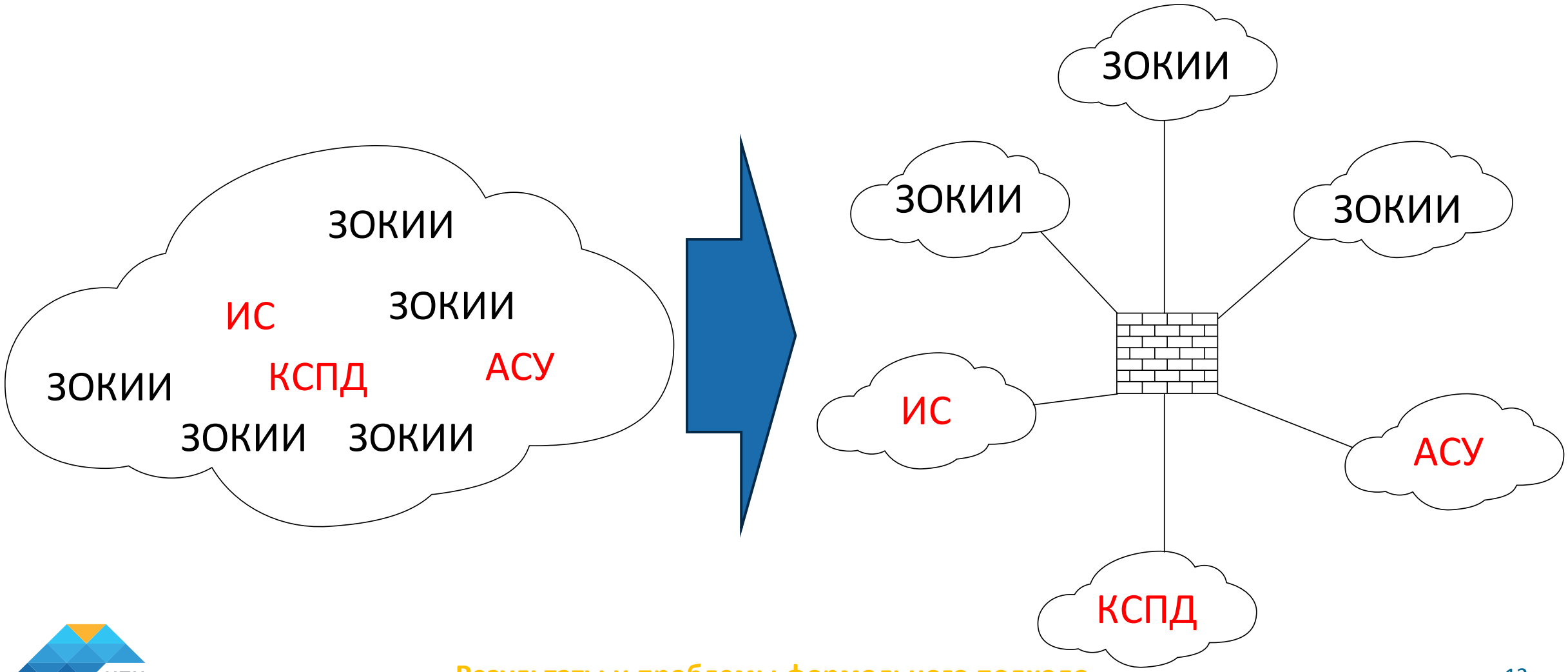
КОНТРОЛЬ СЕТЕВЫХ СОЕДИНЕНИЙ

Состав ИС | Субъекты доступа ИС | **Внешние связи ИС** | Обработка информации | Функции СПО и ППО | Персонал



ОТСУТСТВИЕ СЕГМЕНТАЦИИ СЕТИ

Состав ИС | Субъекты доступа ИС | **Внешние связи ИС** | Обработка информации | Функции СПО и ППО | Персонал



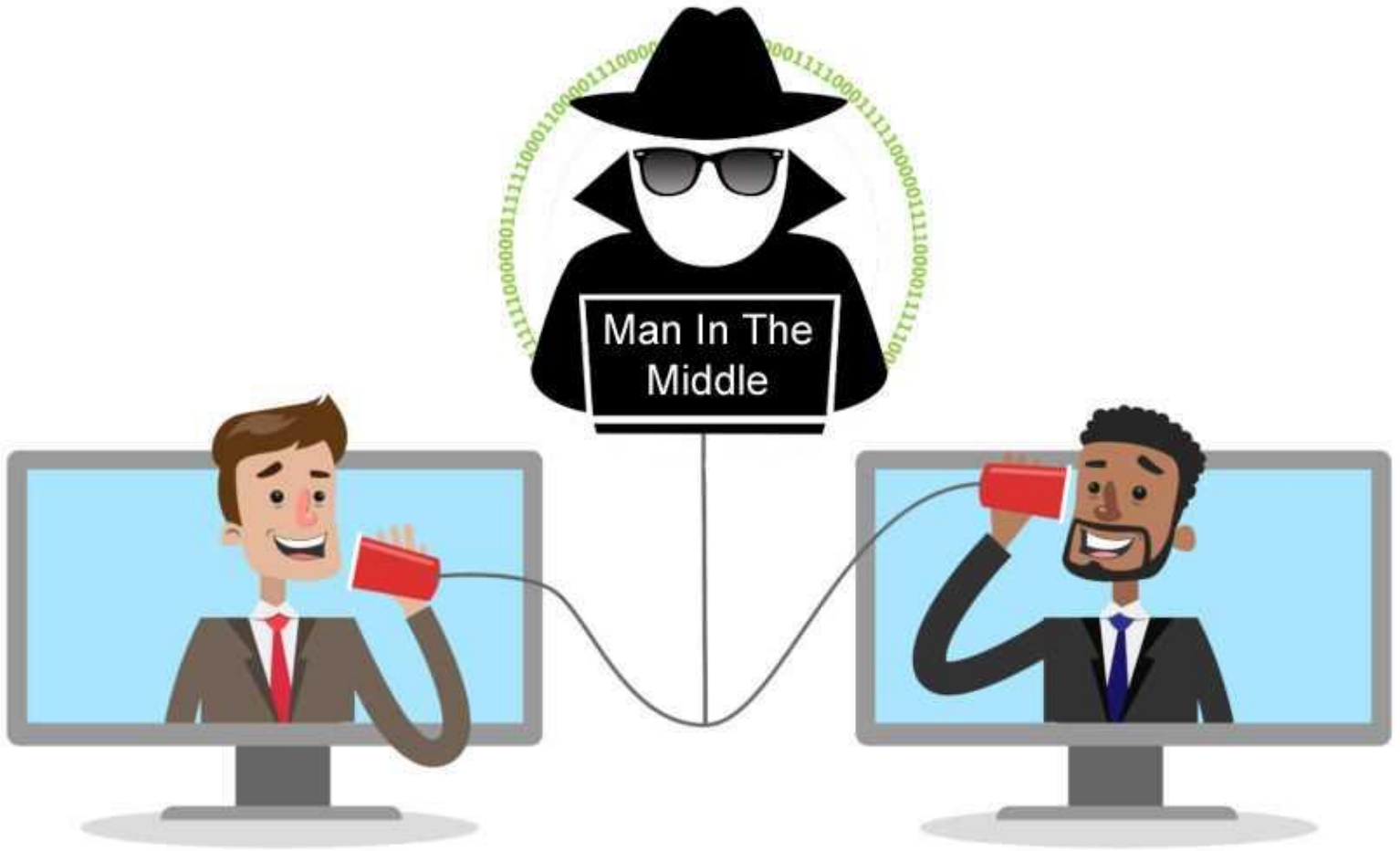
ОТСУТСТВИЕ КОНТРОЛЯ ИНТЕРФЕЙСОВ ВВОДА-ВЫВОДА

Осуществляется контроль
не всех интерфейсов ввода вывода

Контроль входящей информации на предмет:

- ✓ наличия вредоносного кода
- ✓ полноты
- ✓ корректности
- ✓ источника поступления

ИСПОЛЬЗОВАНИЕ ОТКРЫТЫХ ПРОТОКОЛОВ ПЕРЕДАЧИ



НЕПОЛНЫЕ ПРОЦЕССЫ ОБЕСПЕЧЕНИЯ ИБ

Состав ИС | **Субъекты доступа ИС** | **Внешние связи ИС** | **Обработка информации** | **Структура и функции** | **Персонал**

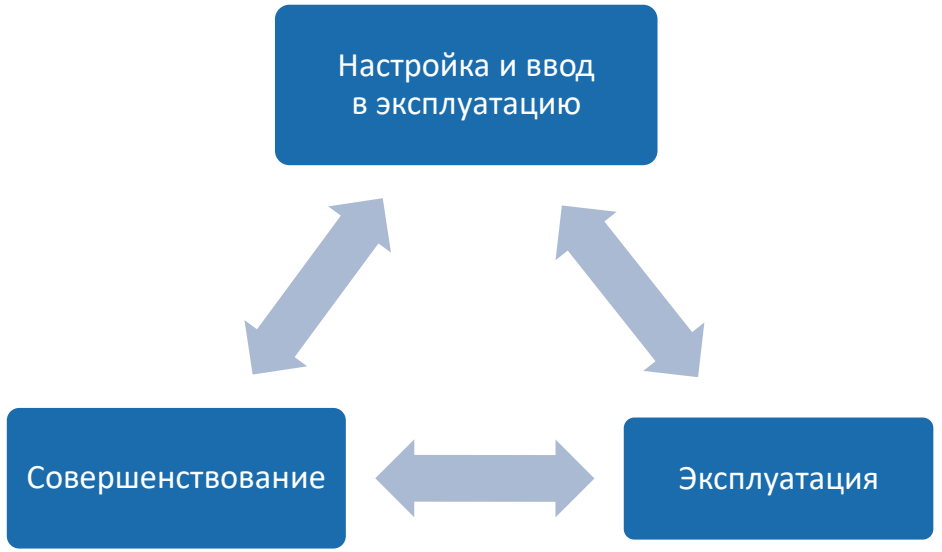
Управление доступом

Информирование и обучения персонала

Антивирусная защита

Обеспечение действий в нештатных ситуациях

Управление конфигурацией



Идентификация и аутентификация

Управление обновлениями ПО

Предотвращение вторжений

Защита машинных носителей информации

Защита ИС и ее компонентов

Защита технических средств и систем

ОСНОВАНО НА ОПЫТЕ

ЧТО ДЕЛАТЬ?

НТЦ ВУЛКАН

ОБЪЕКТЫ ВОЗДЕЙСТВИЯ И ИНСТРУМЕНТЫ

Что делать?

НТЦ ВУЛКАН

ОБЪЕКТЫ КИИ

Всегда оценивать возможность пересмотра границ объектов КИИ для оптимизации расходов на обеспечение безопасности и оптимизации управления.

- Объект КИИ должен содержать инструменты защиты.
- Объект КИИ должен быть подконтрольным – понятные границы, доступность.
- Объект КИИ должен быть «счетным» и «конечным» для инвентаризации.

- Если нет – перекатегорировать.

НТЦ ВУЛКАН

Что делать?

ИНФРАСТРУКТУРА

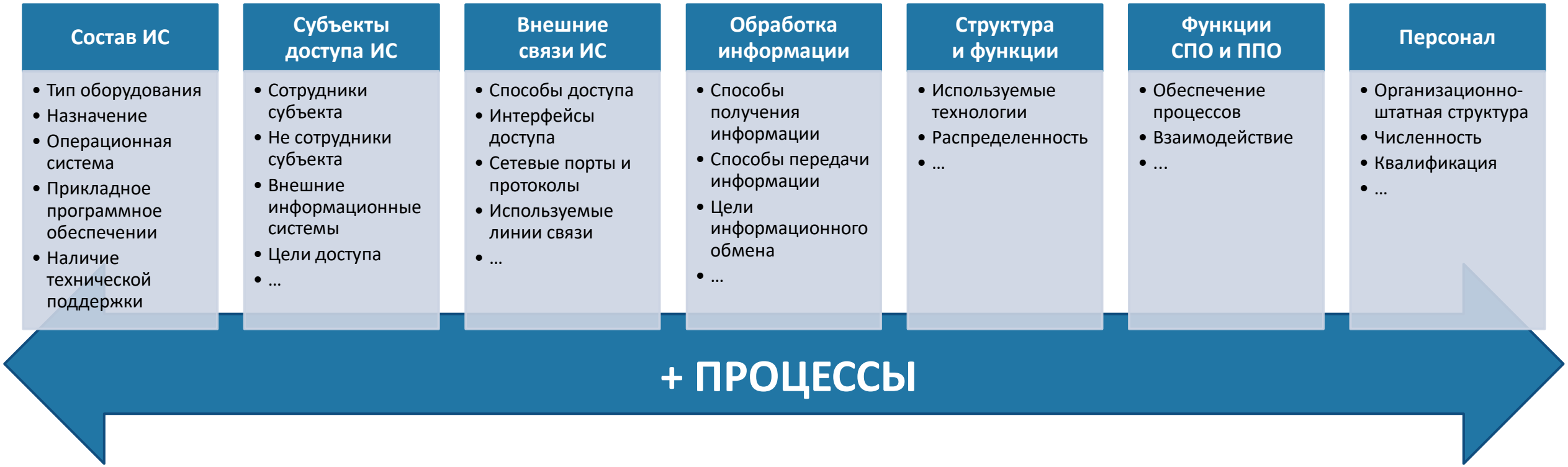
Подходить к выбору программных продуктов и ПАК (импортозамещение) с позиции «как этим пользоваться сейчас и через 5 лет», учитывая полный жизненный цикл.

- Правильное проектирование
- Правильное внедрение
- Правильная поддержка жизненного цикла

ПЕРСОНАЛ

Повышать квалификацию персонала (ИБ и линейный). Работа должна носить системный характер за счет инструментов по автоматизации и распространятся на весь кадровый состав организации.

ПОСТРОЕНИЕ СУИБ - ОБСЛЕДОВАНИЕ



Более 150 метрик !

ПОСТРОЕНИЕ СУИБ - ПРОЕКТИРОВАНИЕ

Что делать?

ВНЕДРЕНИЕ СУИБ – ТЕХНИЧЕСКИЕ СРЕДСТВА

Встроенные средства

- Настройка
- Наличие техподдержки

Наложенные средства

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

НТЦ ВУЛКАН

Что делать?

ВНЕДРЕНИЕ СУИБ - ПРОЦЕССЫ

Что делать?

К ЧЕМУ СТРЕМИТЬСЯ

СОПРОВОЖДЕНИЕ

- Осуществление критического процесса
- Выделение КИИ и категорирование
- Построение системы ИБ
- Ввод системы ИБ в эксплуатацию
- Периодический аудит ИБ
- Модернизация критического процесса

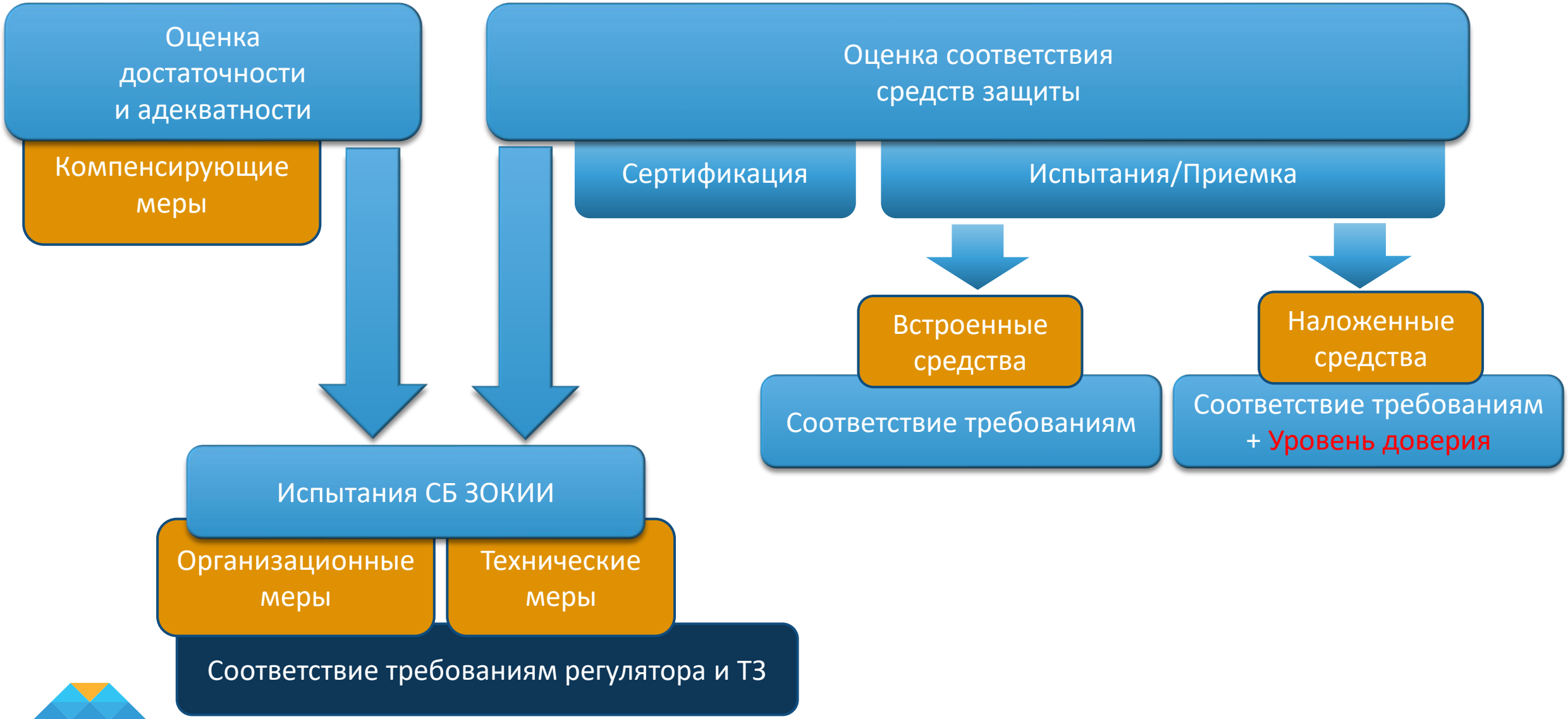
СОПРОВОЖДЕНИЕ: ВЫВОДЫ

- Необходимо реализовать непрерывный цикл сопровождения и поддержания системы безопасности.
- Переход от передачи в промышленную эксплуатацию к налаженной работе должен быть достаточным по времени, чтобы сотрудники ИБ предприятия выработали навыки управления.
- Интегратор может периодически, оценивать состояние и корректировать процессы «по факту».

ПРОВЕРКА РЕГУЛЯТОРА

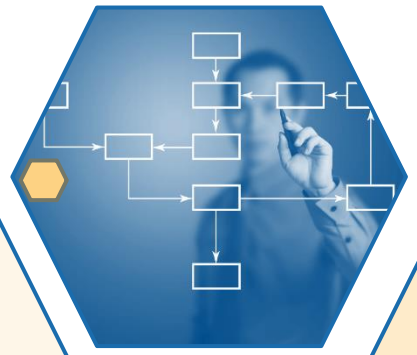
Технические средства	Процессы	ОРД и проектная документация
• Настройка • Достаточность	• Соответствие ОРД • Достаточность • «Следы»	• Соответствие реальной системе • Соответствие требованиям регулятора
Качество проектирования	**Обучение персонала**	**Качество обследования**

ВНЕШНИЙ КОНТРОЛЬ



КОМПЛЕКСНАЯ ЗАЩИТА ЗОКИИ

Реализация процессов
Обеспечение безотказной
повседневной работы



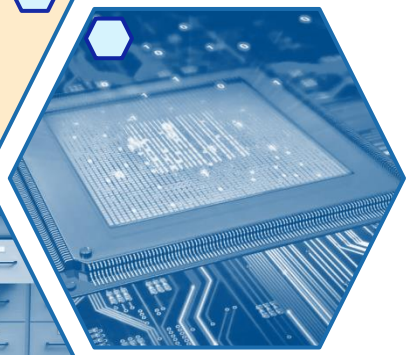
Соответствие
изменяющимся нормам
Возможность противостоять
новым компьютерным атакам

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

ТЕМЫ ДЛЯ ДИСКУССИИ

- Проблемные аспекты ИТ/ИБ-ландшафта предприятий энергетики.
- Типовые проблемы при проектировании СУИБ и требований, включаемых в технические задания на проектирование.
- Типовых проблемы при внедении организационных мер (процессов) управления ИБ.
- Оптимальные пути импортозамещения технических и программных инструментов СУИБ.
- Поддержка СУИБ на протяжении всего жизненного цикла.

НТЦ ВУЛКАН

СПАСИБО ЗА ВНИМАНИЕ!

marketing@ntc-vulkan.ru

НТЦ ВУЛКАН

www.ntc-vulkan.ru