НТЦ ВУЛКАН

Импортозамещение ИТ- и ИБ-инфраструктуры, как окно возможностей для построения оптимальной системы обеспечения безопасности значимых объектов КИИ

Орехов Алексей Юрьевич

Руководитель проектно-технологического управления

09.10.2024

www.ntc-vulkan.ru

КРИТИЧЕСКАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА (КИИ)

Обобщение опыта реализации проектов в следующих отраслях

Правительство Российской Федерации

Президент Российской Федерации

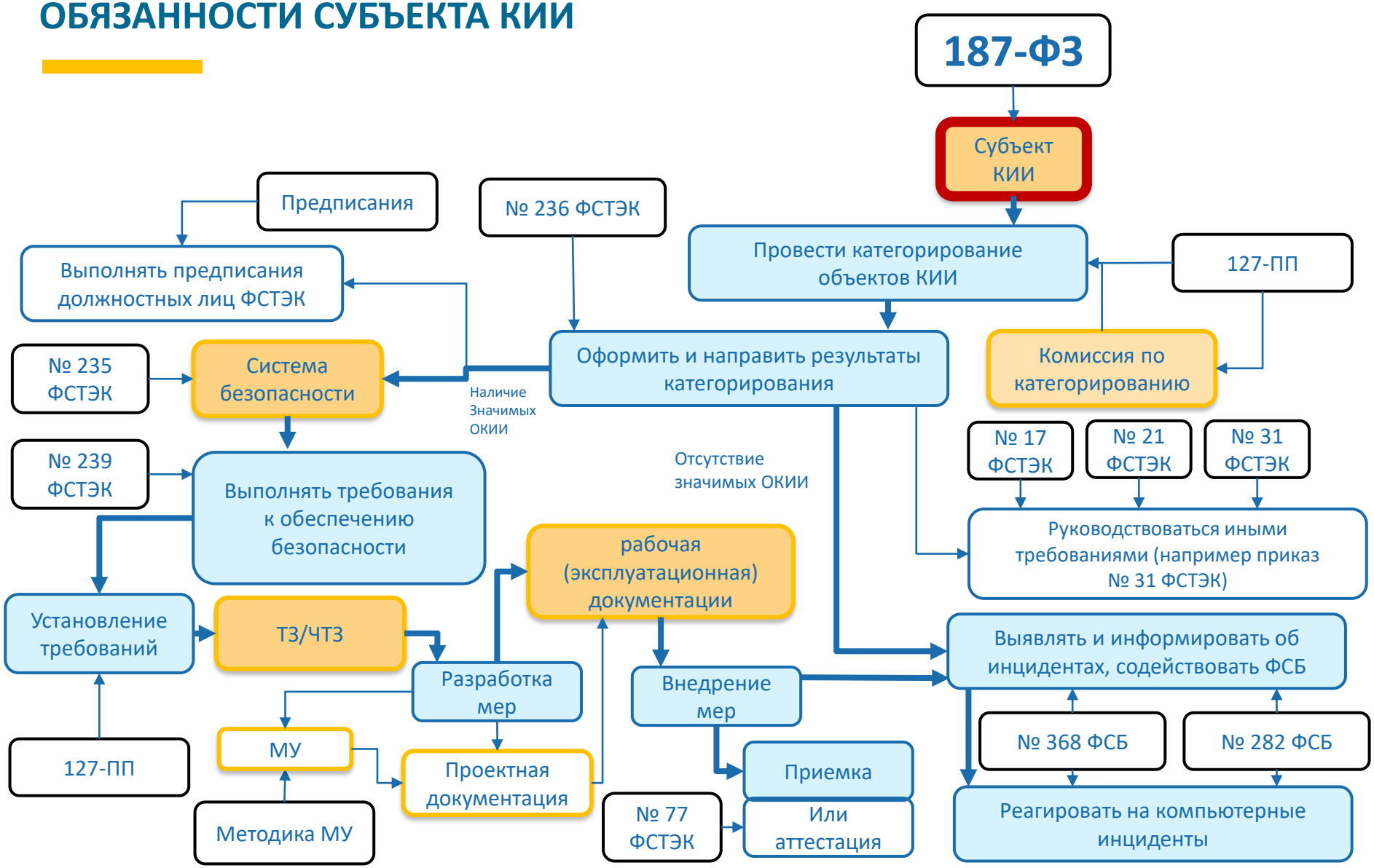
Федеральная служба безопасности Российской Федерации

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации

Федеральная служба по техническому и экспортному контролю Российской Федерации

Банк России

ОБЯЗАННОСТИ СУБЪЕКТА КИИ



КАТЕГОРИРОВАНИЕ ОБЪЕКТОВ КИИ

RG.RU

Правительство предложили наделить правом определять принадлежность к критической инфраструктуре

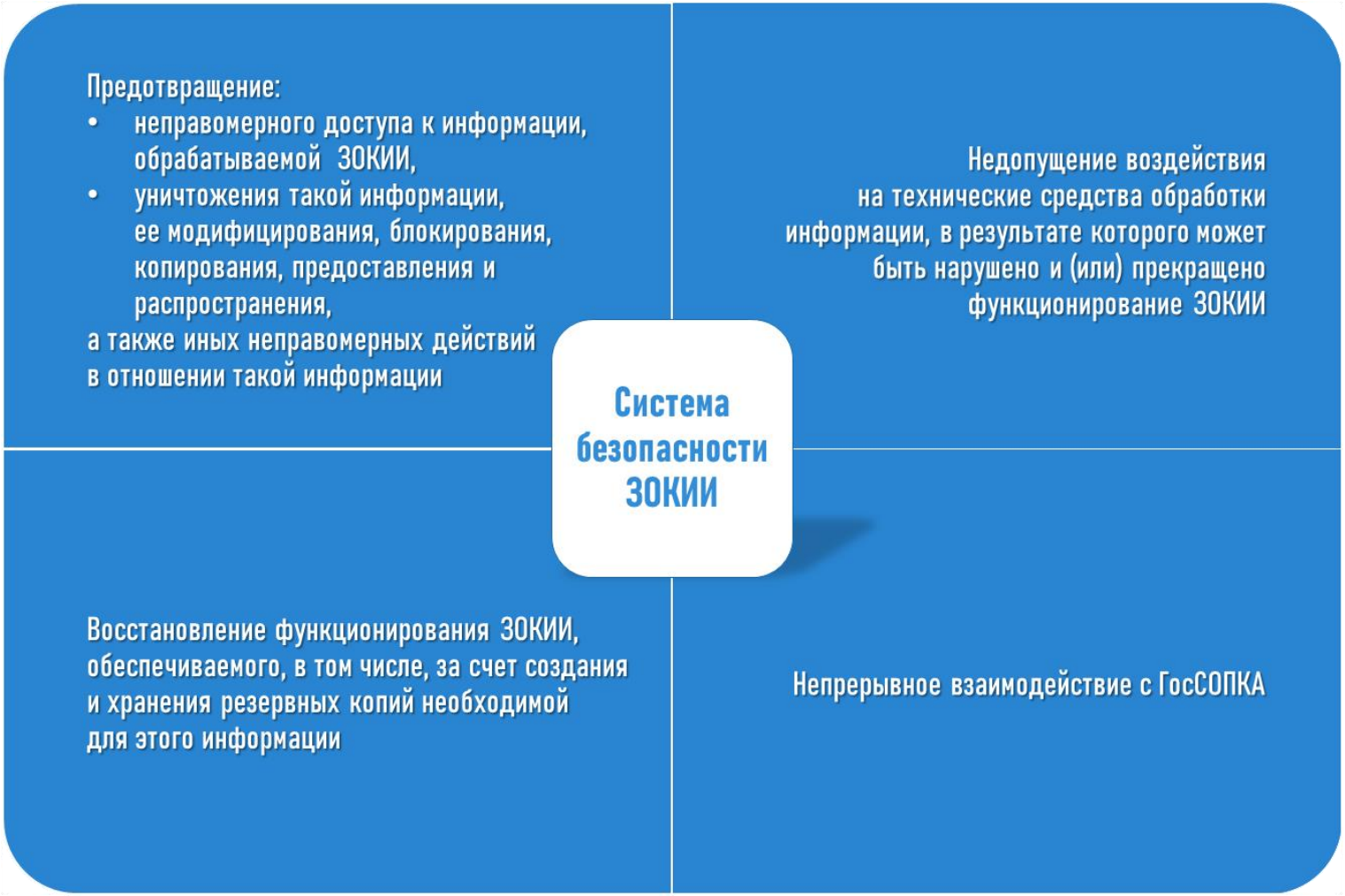
Олег Капранов

Минцифры подготовило предложения по внесению изменений в закон о критической информационной инфраструктуре (КИИ). Соответствующий законопроект внесен в Госдуму. Он наделяет Правительство России полномочиями определять по каждой отрасли типы информсистем, которые необходимо будет относить к значимым объектам КИИ с учетом отраслевых особенностей.

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

ЗАДАЧИ СИСТЕМЫ БЕЗОПАСНОСТИ КИИ



СПЕЦИФИКА ИТ-ИНФРАСТРУКТУРЫ ФИНАНСОВОЙ ОРГАНИЗАЦИИ

- ➔ **Нельзя оперативно перестроить**
- ➔ **ИТ превалирует над ИБ**
- ➔ **Нестандартные ИС**
- ➔ **Слабая связь ИТ и ИБ в части планирования**

ВЫЯВЛЯЕМЫЕ ПРОБЛЕМЫ

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

На разных этапах жизненного цикла

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

НЕВЕРНОЕ ОПРЕДЕЛЕНИЕ ГРАНИЦ ЗОКИИ

Границы ЗОКИИ	Права доступа	Управление идентификаторами	Сегментация сети	Контроль соединений	Интерфейсы ввода-вывода	Открытые протоколы	Процессы ИБ

«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

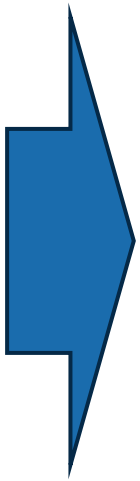
- Появление множества взаимодействующих ИС
- «Разрыв» технологического (критического) процесса

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

«ПЛОСКИЕ» ПРАВА ДОСТУПА В ЗОКИИ

Границы ЗОКИИ	Права доступа	Управление идентификаторами	Сегментация сети	Контроль соединений	Интерфейсы ввода-вывода	Открытые протоколы	Процессы ИБ

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



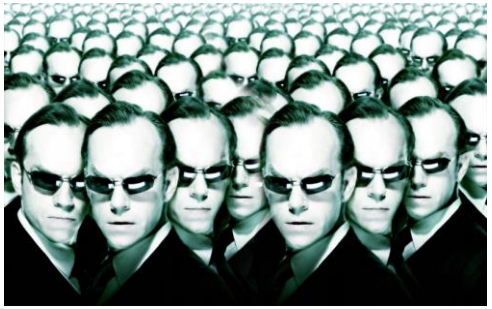
- ✓ Разграничение прав доступа встроенными механизмами
- ✓ «Терминирование» доступа
- ✓ Использование PAM-систем

ОТСУТСТВИЕ УПРАВЛЕНИЯ ИДЕНТИФИКАТОРАМИ/АУТЕНТИФИКАТОРАМИ

Границы ЗОКИИ | Права доступа | **Управление идентификаторами** | Сегментация сети | Контроль соединений | Интерфейсы ввода-вывода | Открытые протоколы | Процессы ИБ

Top 20 паролей

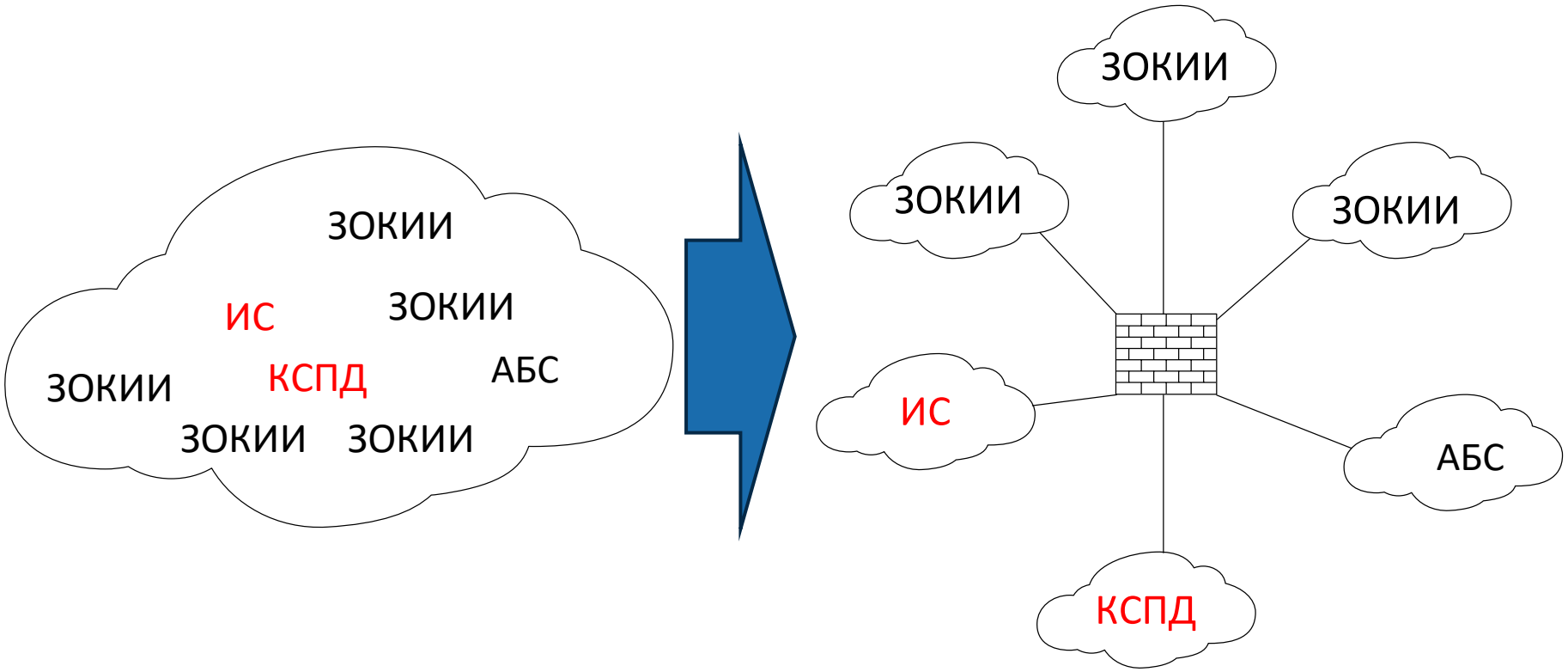
Gmail	Yandex	Mail.ru
123456	123456	qwerty
password	123456789	123456
123456789	111111	qwertyuiop
qwerty	qwerty	qwe123
12345678	1234567890	qweqwe
111111	1234567	klaster
abc123	7777777	1qaz2wsx
123123	123321	1q2w3e4r
1234567	000000	qazwsx
1234567890	123123	1q2w3e
iloveyou	666666	123qwe
password1	12345678	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)

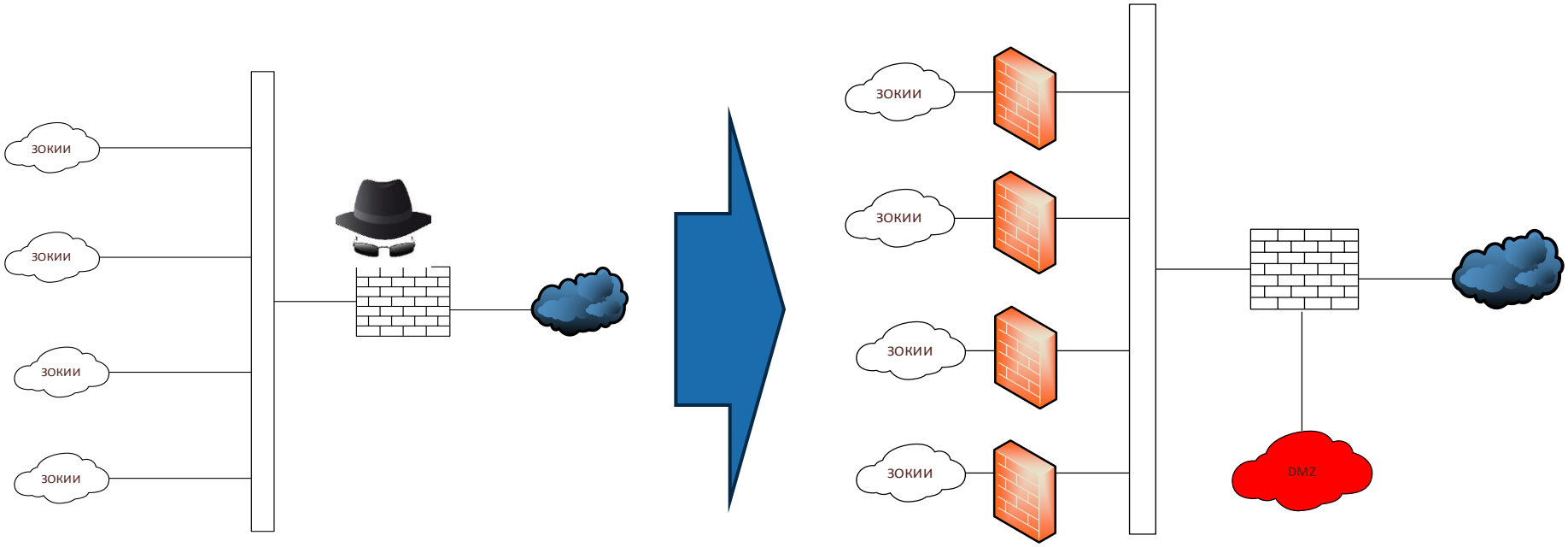
НЕВЕРНАЯ СЕГМЕНТАЦИИ СЕТИ

Границы ЗОКИИ	Права доступа	Управление идентификаторами	Сегментация сети	Контроль соединений	Интерфейсы ввода-вывода	Открытые протоколы	Процессы ИБ



КОНТРОЛЬ СЕТЕВЫХ СОЕДИНЕНИЙ

Границы ЗОКИИ | Права доступа | Управление идентификаторами | Сегментация сети | **Контроль соединений** | Интерфейсы ввода-вывода | Открытые протоколы | Процессы ИБ



ОТСУТСТВИЕ КОНТРОЛЯ ИНТЕРФЕЙСОВ ВВОДА-ВЫВОДА

Границы ЗОКИИ	Права доступа	Управление идентификаторами	Сегментация сети	Контроль соединений	Интерфейсы ввода-вывода	Открытые протоколы	Процессы ИБ

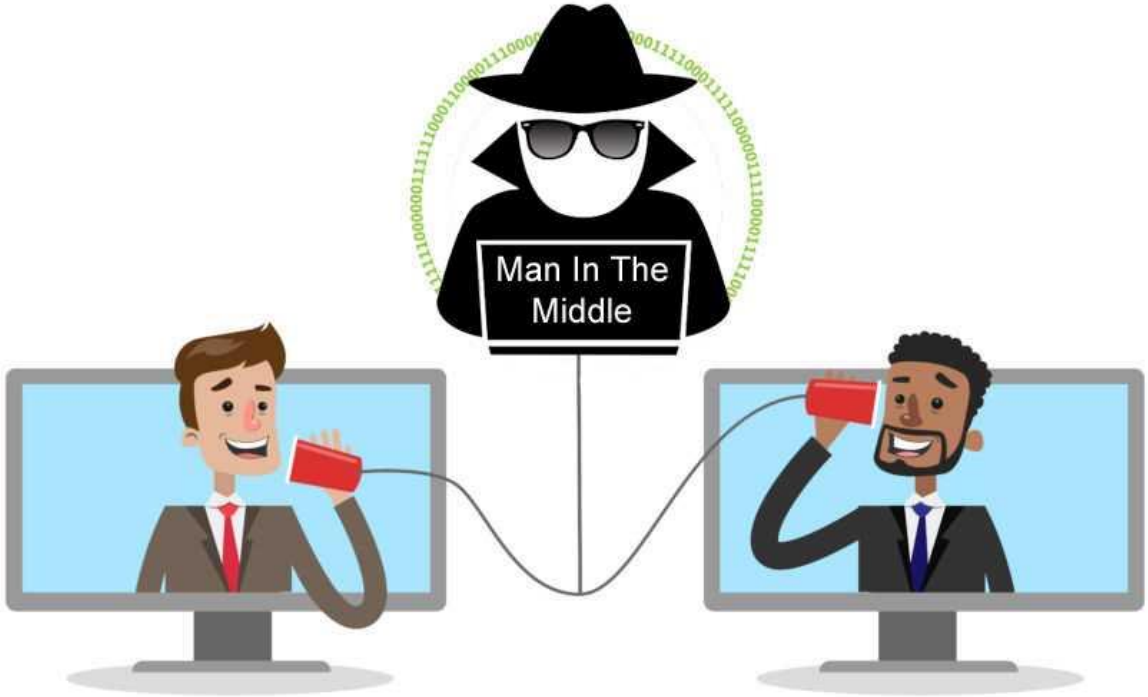
Осуществляется контроль
не всех интерфейсов ввода вывода

Контроль входящей информации на предмет:

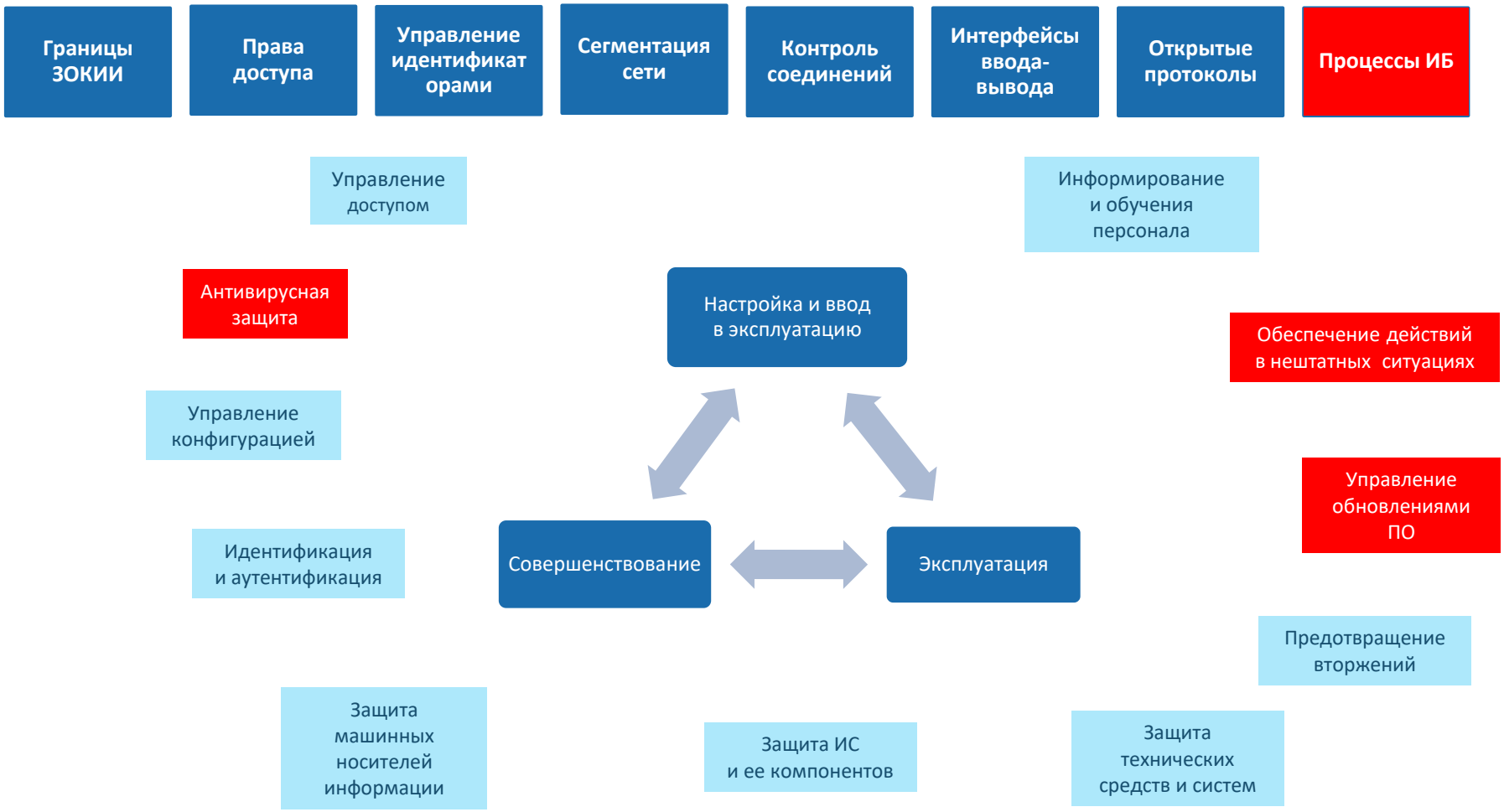
- ✓ наличия вредоносного кода
- ✓ полноты
- ✓ корректности
- ✓ источника поступления

ИСПОЛЬЗОВАНИЕ ОТКРЫТЫХ ПРОТОКОЛОВ ПЕРЕДАЧИ

Границы ЗОКИИ	Права доступа	Управление идентификаторами	Сегментация сети	Контроль соединений	Интерфейсы ввода-вывода	**Открытые протоколы**	Процессы ИБ



НЕПОЛНЫЕ ПРОЦЕССЫ ОБЕСПЕЧЕНИЯ ИБ



ИМПОРТОЗАМЕЩЕНИЕ ИТ- И ИБ-ИНФРАСТРУКТУРЫ

«окно возможностей»

- Повысить квалификацию и статус ИБ-подразделений при принятии решений
- Перестроить процессы ИБ и автоматизировать их
- Перепроектировать системы в целом с учетом потребностей ИБ

СИЛЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ (235 приказ ФСТЭК)

Структурное подразделение по безопасности ЗОКИИ
и/или
специалисты по безопасности ЗОКИИ

Функции:

- разрабатывать предложения по совершенствованию ОРД и представлять их руководителю субъекта КИИ
- проводить анализ УБИ в отношении ЗОКИИ и выявлять уязвимости в них
- обеспечивать реализацию требований по обеспечению безопасности ЗОКИИ
- обеспечивать реализацию организационных мер и применение средств защиты информации, эксплуатацию средств защиты информации
- осуществлять реагирование на компьютерные инциденты организовывать проведение оценки соответствия ЗОКИИ требованиям по безопасности
- готовить предложения по совершенствованию функционирования СБ ЗОКИИ, а также по повышению уровня безопасности ЗОКИИ

Требования:

- **К руководителю подразделения** –
  высшее профессиональное образование в области ИБ или завершенная программа профессиональной переподготовки по направлению «Информационная безопасность» (со сроком обучения не менее 360 часов), наличие стажа работы в сфере ИБ не менее 3 лет
- **К штатным работникам подразделения** –
  высшее профессиональное образование в области ИБ или завершенное обучение по программе повышения квалификации по направлению «Информационная безопасность» (со сроком обучения не менее 72 часов)
- **Ко всем работникам** –
  прохождение не реже одного раза в 5 лет обучения по программам повышения квалификации по направлению «Информационная безопасность»

Острая потребность в дополнительных ресурсах

ПРОЦЕССЫ ОБЕСПЕЧЕНИЯ ИБ И ИМПОРТОЗАМЕЩЕНИЕ

Для обеспечения непрерывности процессов ИБ необходима
перестройка цепочки принятия решений в рамках цифровизации и импортозамещения

Процессы	По документам	Фактически
Антивирусная защита	АВ закуплены и установлены, ежегодно приобретается поддержка	ПО не установлено, либо имеет урезанный функционал
Обеспечение действий в нештатных ситуациях	Написаны и лежат в папках инструкции для персонала	Инструкция не применима, т.к. произошла замена ПО и инфраструктуры
Идентификация и аутентификация	Приказом регламентированы «сложные» пароли	qwe123, 12345678 …
Защита машинных носителей информации	Существуют журналы доверенных носителей	Произошел переход на платформу виртуализации

и многое другое...

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

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

КОМАНДНАЯ ИГРА - ИТ, ИБ И БИЗНЕС

ВЫДЕЛЕНИЕ ОКИИ И КАТЕГОРИРОВАНИЕ

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.

ИТ- и ИБ-ИНФРАСТРУКТУРА

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

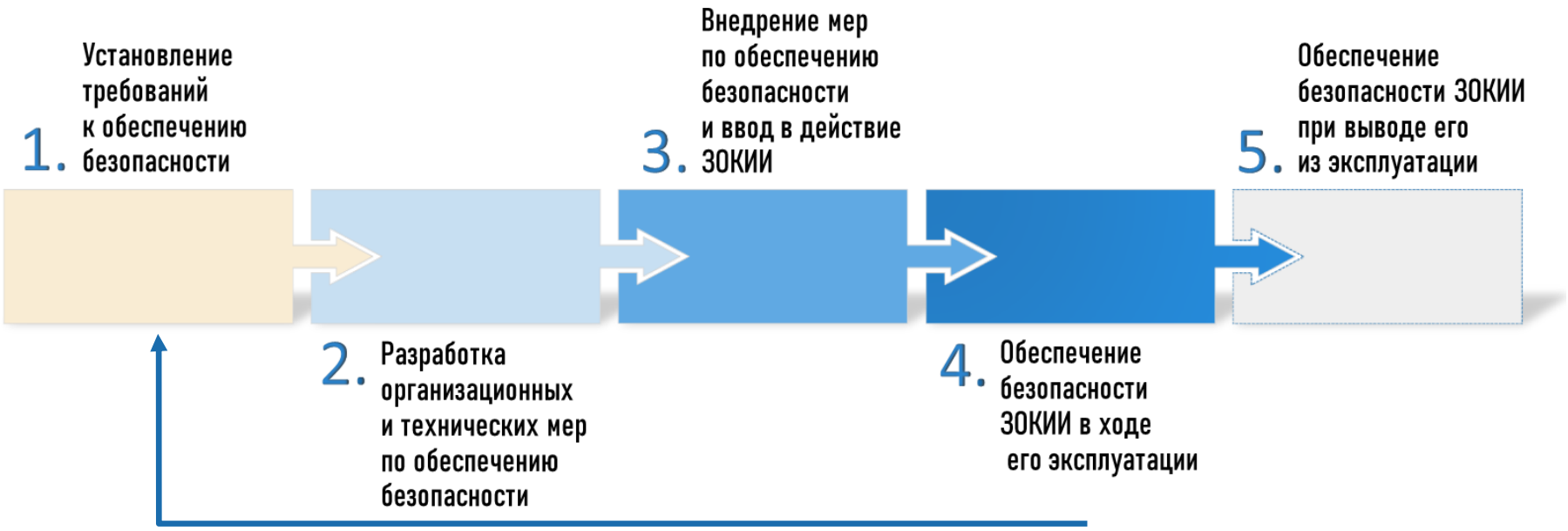
- Правильное проектирование с учетом потребностей ЗОКИИ
- Правильное внедрение с учетом совместимости с процессами ИБ
- Правильная поддержка жизненного цикла с учетом планов развития Бизнеса, ИБ и ИТ

ПЕРСОНАЛ

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

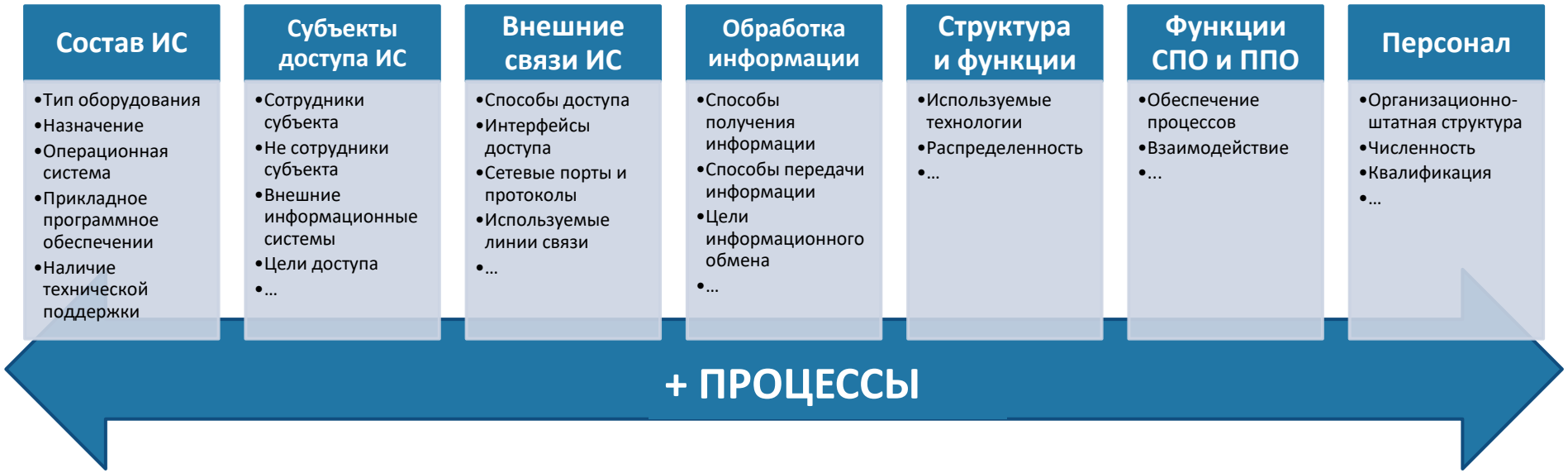
ЖИЗНЕННЫЙ ЦИКЛ

Жизненный цикл реализации требований обеспечения безопасности



ОБЪЕКТЫ ВОЗДЕЙСТВИЯ И ИНСТРУМЕНТЫ

ПОСТРОЕНИЕ СУИБ - ОБСЛЕДОВАНИЕ



Более 150 метрик !

ПОСТРОЕНИЕ СУИБ - ПРОЕКТИРОВАНИЕ

ВНЕДРЕНИЕ СУИБ – ТЕХНИЧЕСКИЕ СРЕДСТВА

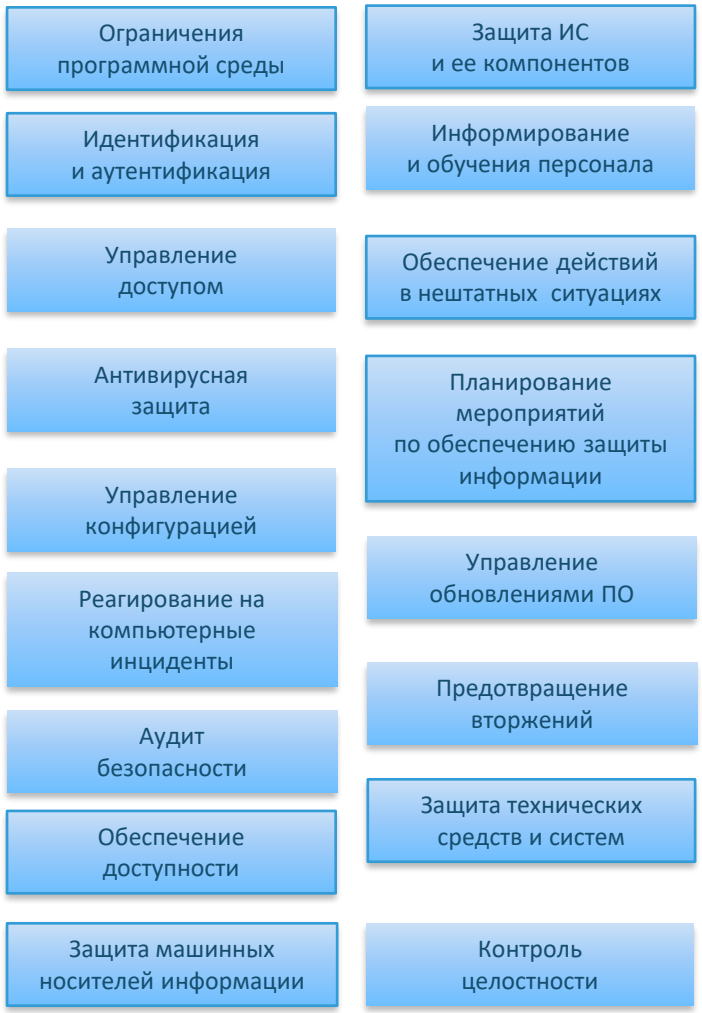
Встроенные средства

- Настройка
- Наличие техподдержки

Наложенные средства

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

ВНЕДРЕНИЕ СУИБ - ПРОЦЕССЫ



ГОСТ Р 57580.1-2017

- Процесс 1 «Обеспечение защиты информации при управлении доступом
- Процесс 2 «Обеспечение защиты вычислительных сетей»
- Процесс 3 «Контроль целостности и защищенности информационной инфраструктуры»

Процесс 4 «Защита от вредоносного кода».

Процесс 5 «Предотвращение утечек информации».

Процесс 6 «Управление инцидентами защиты информации»

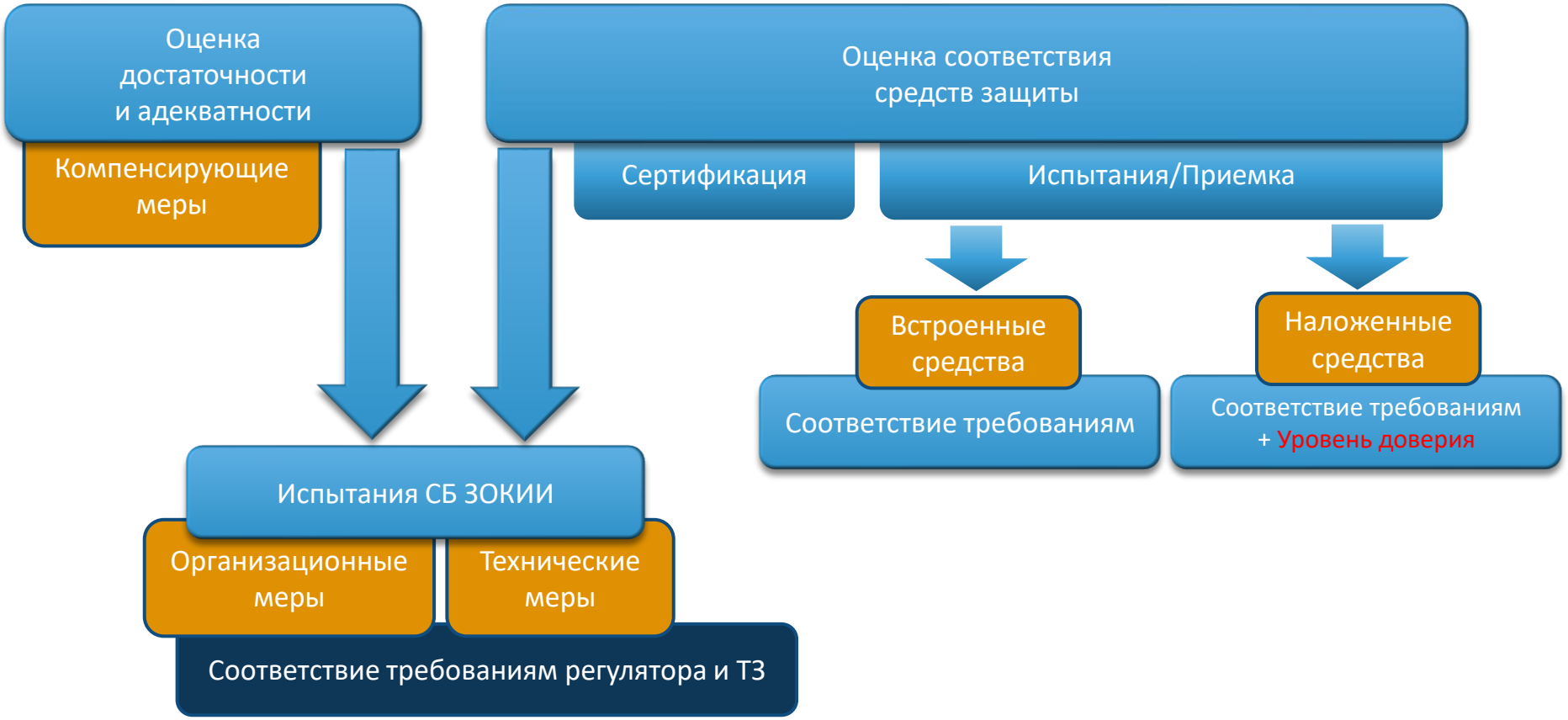
- Процесс 7 «Защита среды виртуализации».

Процесс 8 «Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств»

НТЦ ВУЛКАН

К ЧЕМУ СТРЕМИТЬСЯ

ВНЕШНИЙ КОНТРОЛЬ



КОМПЛЕКСНАЯ ЗАЩИТА ЗОКИИ

ТЕМЫ ДЛЯ ДИСКУССИИ

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

СПАСИБО ЗА ВНИМАНИЕ!

marketing@ntc-vulkan.ru

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