КЗИ 2026

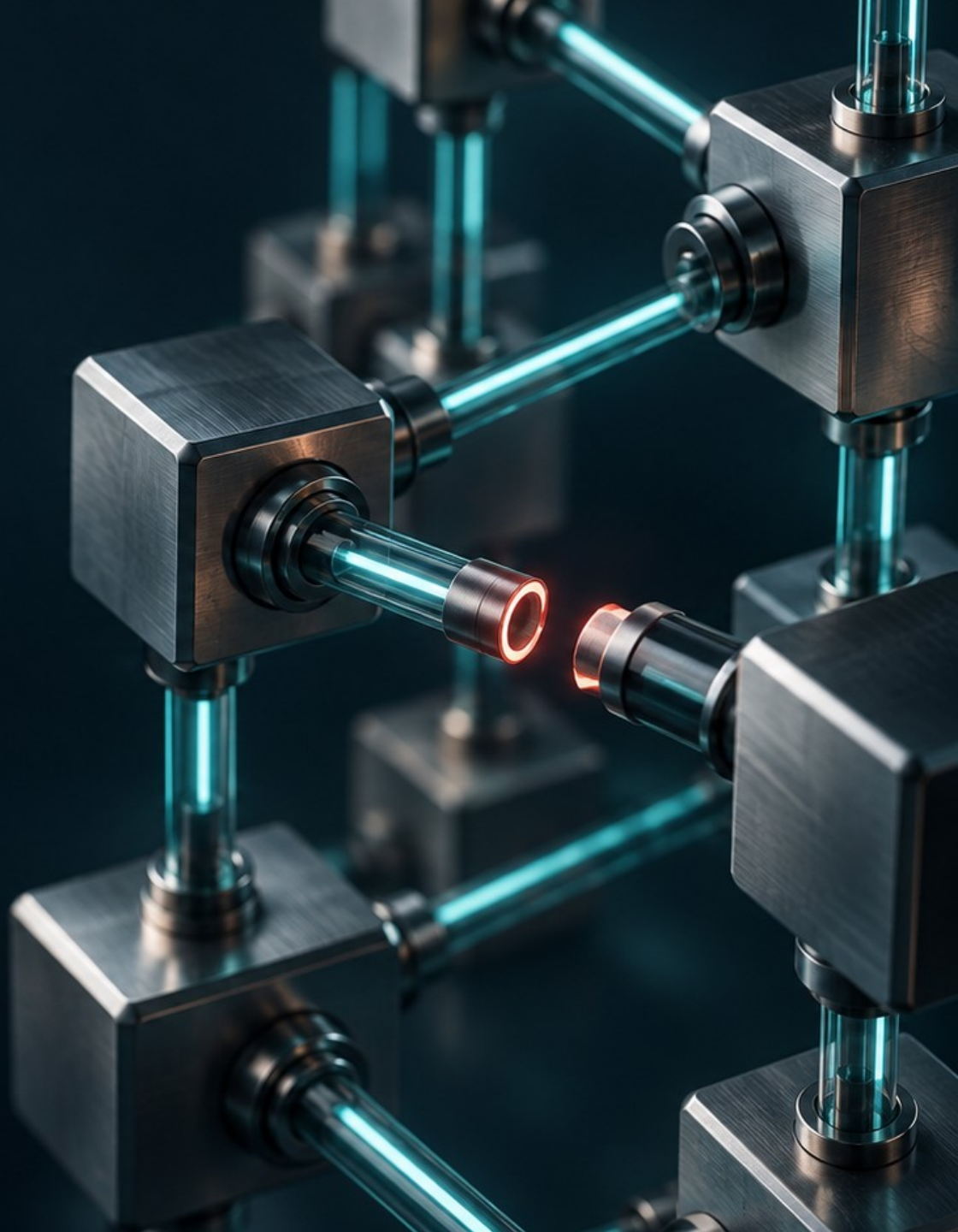
Средства защиты есть.

Защиты нет.

От набора продуктов
к киберустойчивой системе
защиты информации

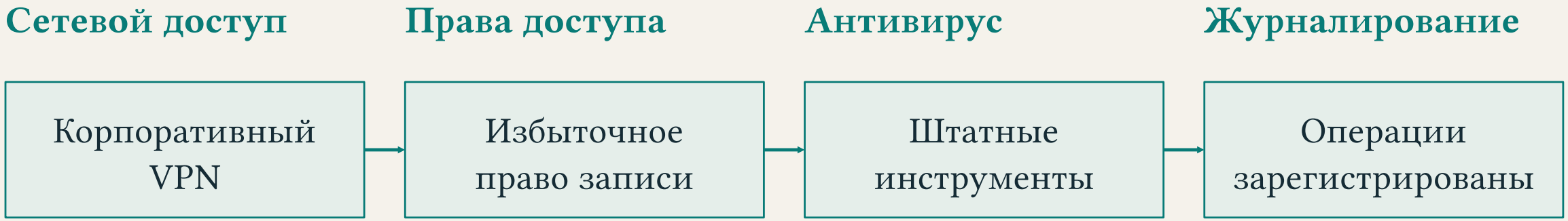
Грязина Софья Вадимовна

ООО «Дженезис Системс», Республика Беларусь, г. Минск



Компрометация пользовательского доступа

Условная инфраструктура: рабочие места, серверы и средства защиты



Рабочие данные изменены или удалены

Проверка: права на данные и действия после подозрительного события

Уровни оценки защиты

Уровень	Основание вывода	Что проверяется на объекте
Средство защиты	Сертификат и условия применения	Применение в нашей инфраструктуре
Мера защиты	Правила, настройки и порядок работы	Все нужные ресурсы и способы доступа
Результат защиты	Контрольные действия и протокол	Ограничение угрозы в заданных условиях

Свойства продукта и результат его применения требуют своих оснований

Разрывы между мерами защиты

Границы

Проверка охватила
не все ресурсы

Зависимости

Общие полномочия
затрагивают разные меры

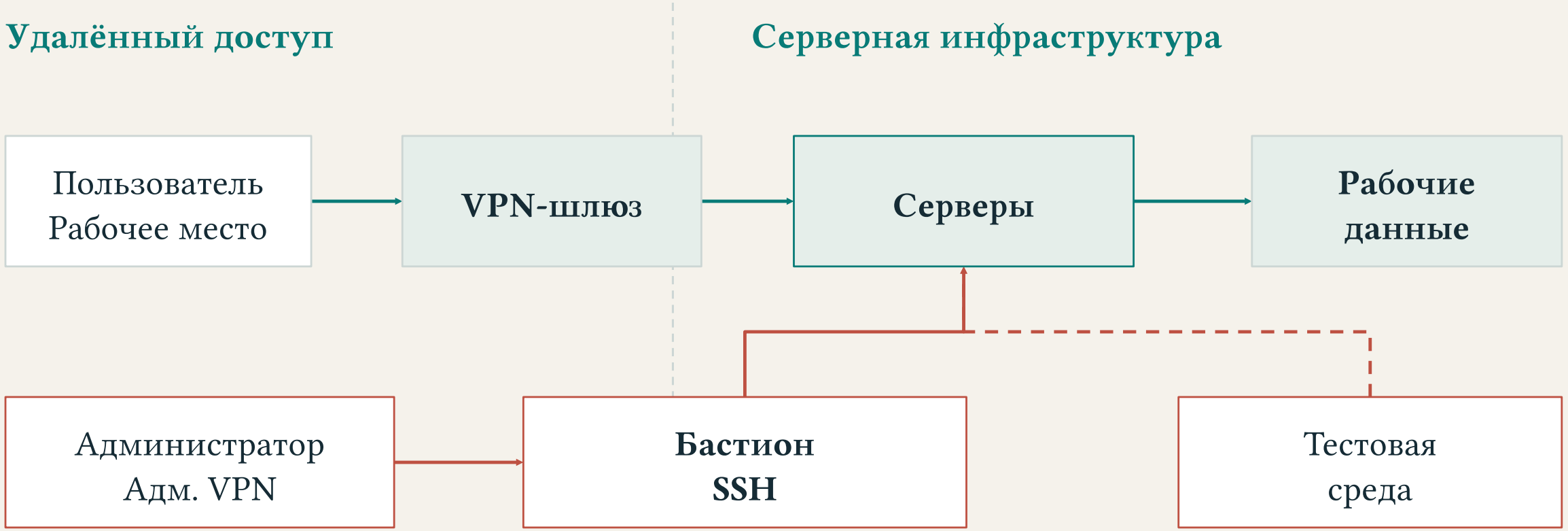
Переключения

Настройки при переходе
могут различаться

Реагирование

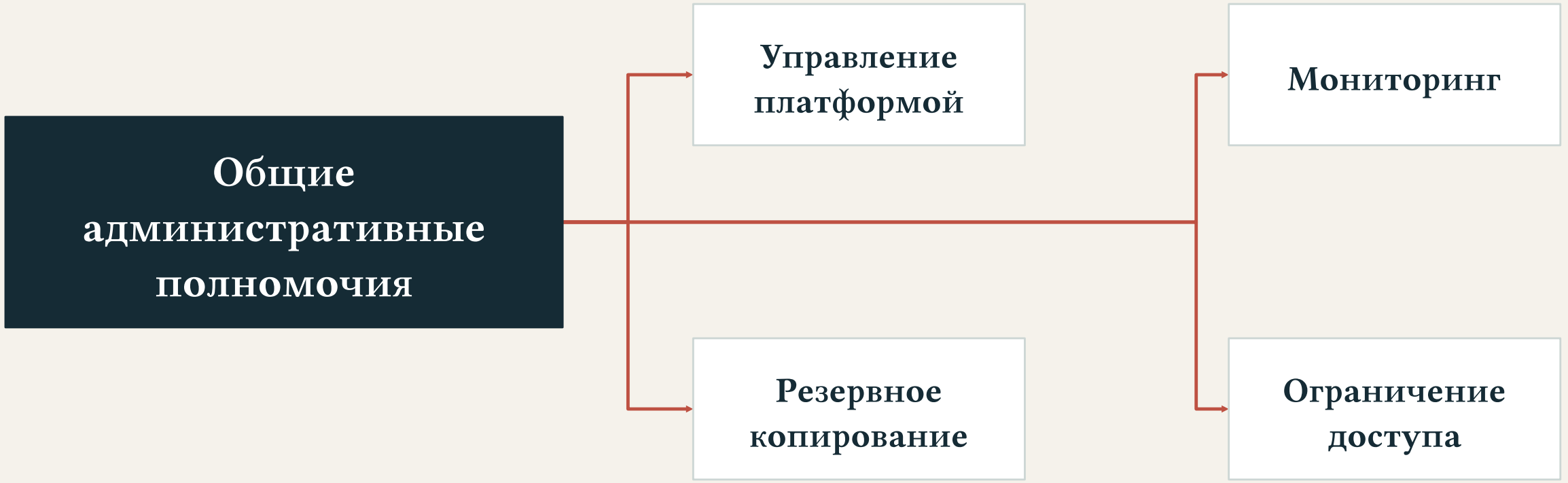
Событие зарегистрировано
Ответственный не определён

Доступ к серверам и данным



Проверка: разрешённые соединения, полномочия и доступ к копиям данных

Общие административные полномочия



Одна запись может влиять на данные, мониторинг и резервные копии

Защита в разных режимах работы

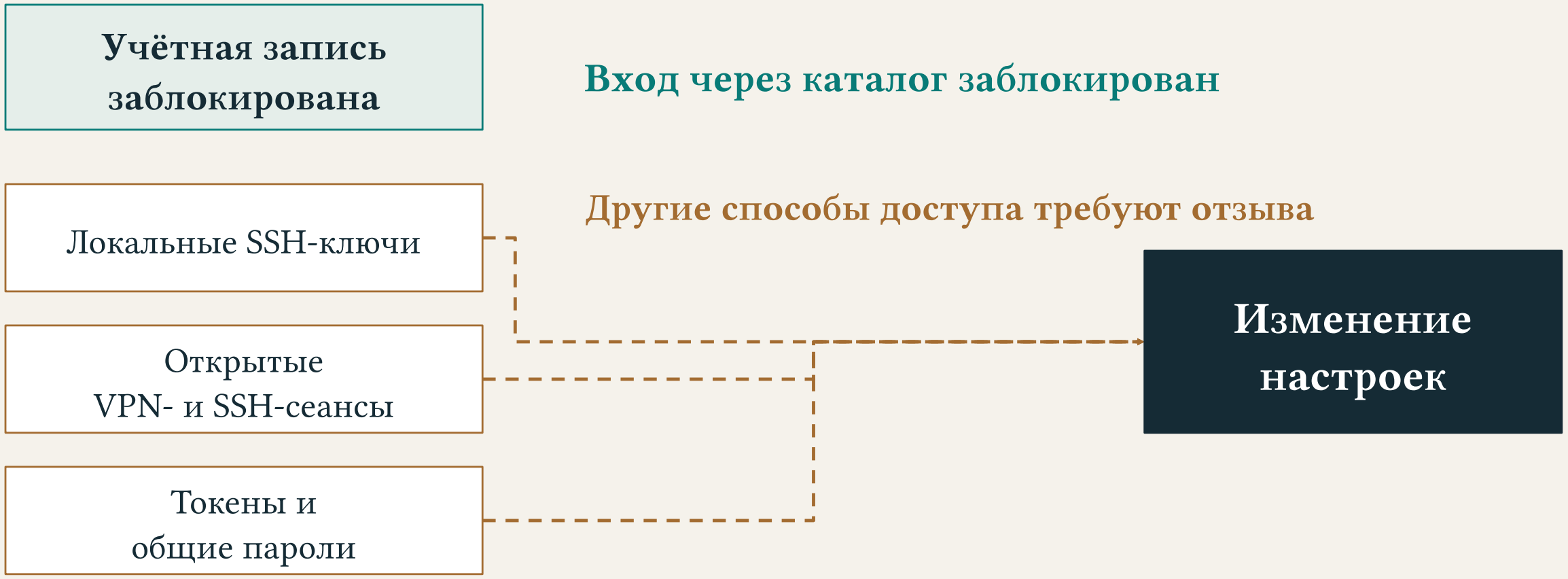
Режим	Что меняется	Что проверяется
Штатный	Рабочий доступ к серверам	Разрешённые соединения и права
Резервный	Резервный VPN-шлюз	Правила доступа и отправка событий
Переходный	Перенос серверов	Временные правила и прежний доступ
Аварийный	Дополнительные права	Регистрация действий и отзыв прав

Проверка охватывает настройки и режимы, указанные в её материалах

Прослеживаемость требований

От требования можно перейти к настройке и результату её проверки

Полный отзыв административного доступа



Проверка включает новые подключения и ранее открытые сеансы

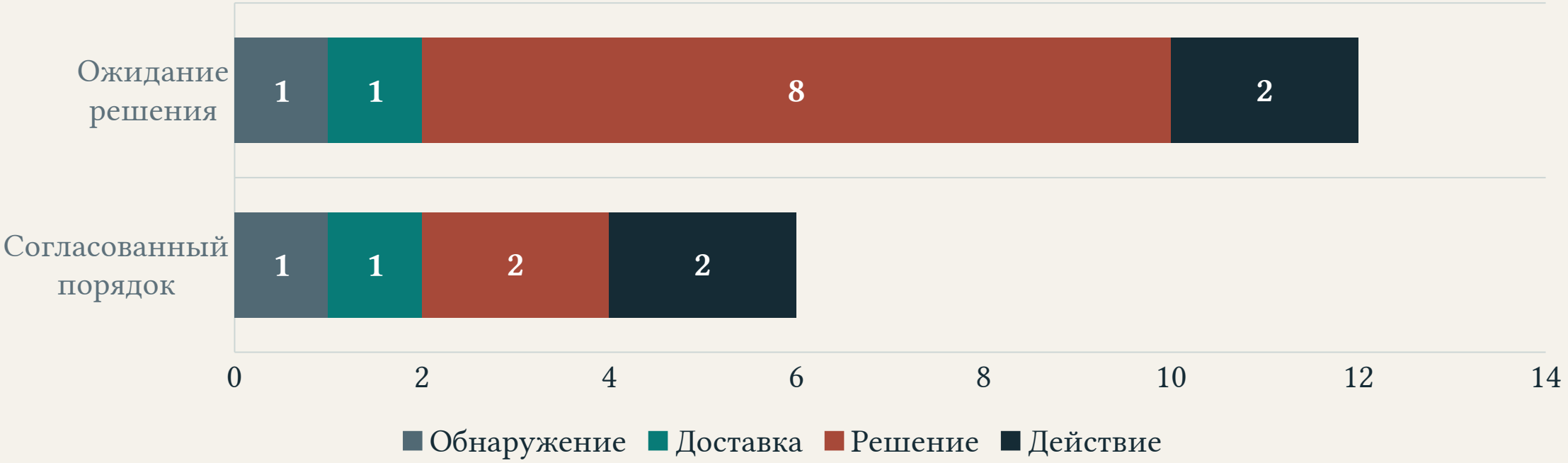
Матрица требований и проверок

Результат	Проверка	Подтверждение	Пересмотр
Доступ отозван	Ключи, открытые сеансы и токены	Настройки прав и протокол	Новый способ администрирования
Инцидент локализован	Ограничение доступа и повторная операция	Время и результат контрольного действия	Изменение обработки событий
Работа восстановлена	Доступ к данным и рабочая операция	Протокол, RTO и RPO	Перенос серверов

Пример структуры записи. Подтверждение относится к проверенным настройкам

Время до локализации инцидента

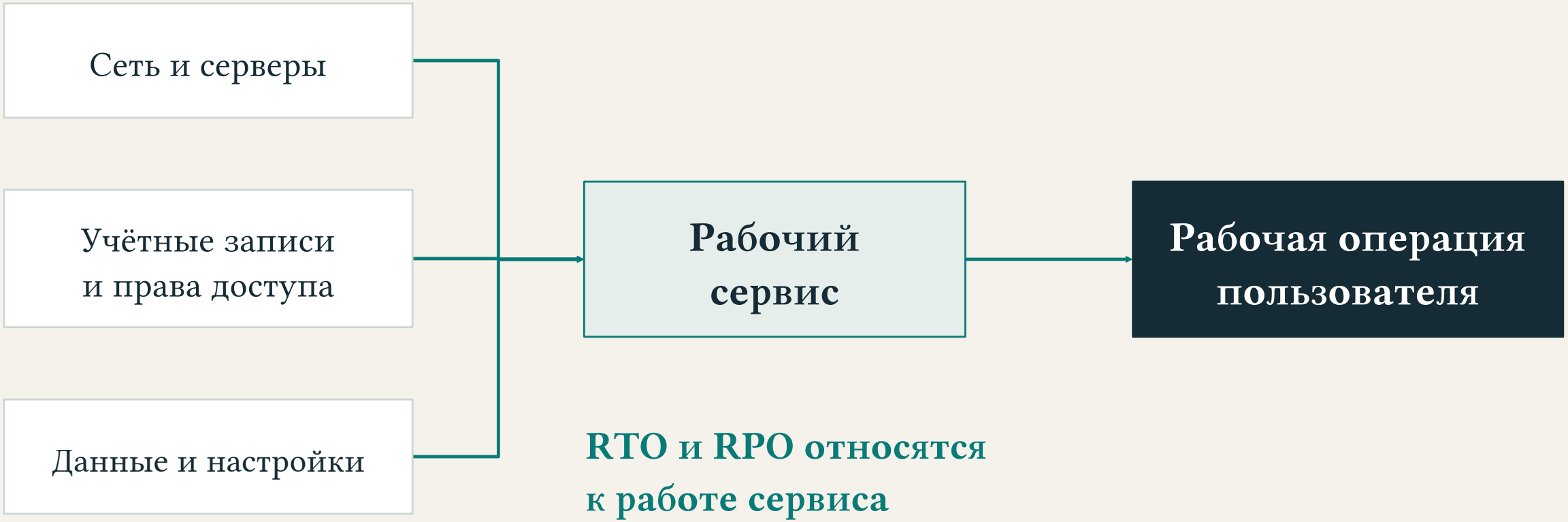
Оба варианта доставляют уведомление через 2 минуты



Локализация: 6 и 12 минут

Расчётный пример. Все интервалы условные, единица измерения: минута

Восстановление работы



Восстановление завершается проверкой рабочей операции

Роль аттестации

Требования
Границы объекта
Условия эксплуатации

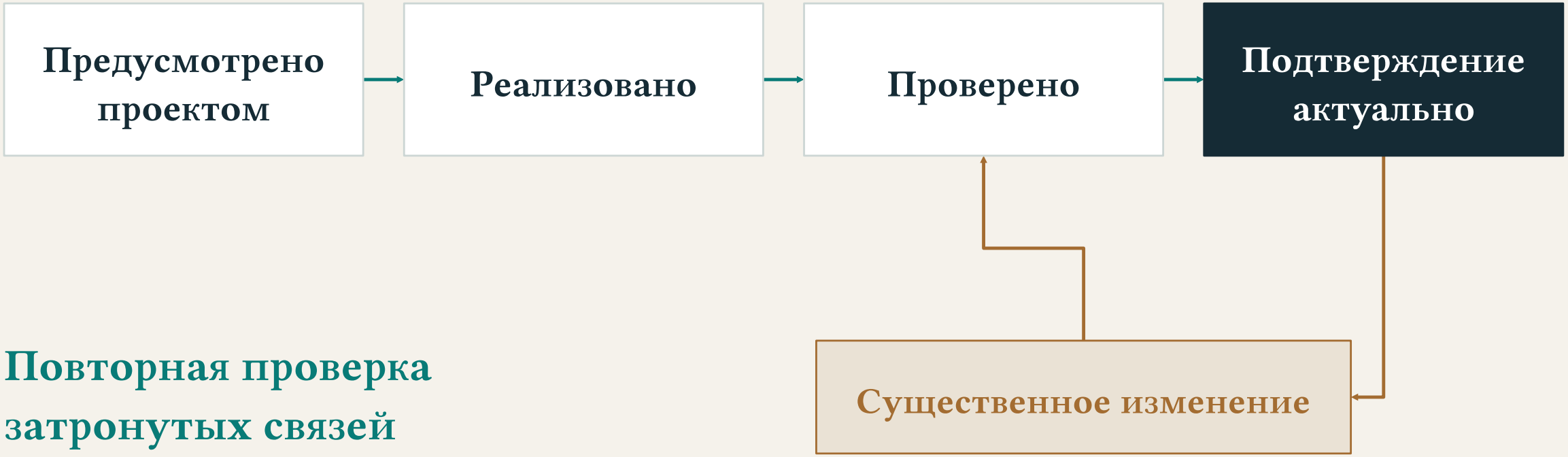
Настройки
Порядок работы
Ответственность

Критерии
Результаты проверок
Условия вывода

Вывод о соответствии в установленных условиях

Беларусь: приказ ОАЦ № 66. Россия: приказ ФСТЭК № 77

Защита после изменений



Повторная проверка затронутых связей

После изменения проверяют связанные требования и настройки

Приоритет проверок

	Недостаточное подтверждение	Достаточное подтверждение
Тяжелые последствия	**Первая очередь проверки**	**Контроль изменений**
Меньшие последствия	**План проверок**	**Поддержание конфигурации**

Авторская схема очередности. Обязательные требования выполняются полностью

Какой ущерб мы ограничим при реализации угрозы?

Чем подтверждено восстановление работы?

Грязина Софья Вадимовна
ООО «Дженезис Системс»

Нормативные основания и область применения

Документ	Предмет	Область применения
Приказ ОАЦ № 66 20.02.2020	Создание и аттестация СЗИ	Ограниченная информация, не отнесённая к государственным секретам
Приказ ФСТЭК № 77 29.04.2021	Аттестация объекта в условиях эксплуатации	Перечень объектов и основания аттестации определены порядком
Методика ФСТЭК 05.02.2021	Последствия и сценарии реализации угроз	Применимость определяется назначением системы и положениями методики

Применимые редакции и состав работ уточняются для конкретного объекта

Вопросы для обсуждения

Вопрос	Основание ответа
Полнота проверки	Границы объекта, угрозы и режимы работы. Ограничения отражают в выводе
Роль матрицы	Связь требования с настройками и протоколом. Обязательные работы определяет применимый порядок
Критерий результата	Доступ прекращён, воздействие ограничено, рабочая операция восстановлена в пределах RTO и RPO
Пересмотр	Влияние изменения на требования и повторная проверка связанных настроек