01 / ОБЛАСТЬ И СМЫСЛ

От наблюдения к понятному решению

Демонстрационный отчёт по вымышленному сервису документов. Этот материал показывает формат и не подтверждает проведение реального аудита.

Границы → **Доказательство** → **Исправление**

Учебный контур

Объект	Искусственный кабинет «Учебный сервис». Реальный адрес отсутствует.
Участники	Две тестовые организации, пользователь и руководитель каждой.
Данные	Документы с явными маркерами ПРИМЕР-А и ПРИМЕР-Б, без персональных сведений.
Цель	Показать, как описывается правило принадлежности документа и критерий повторной проверки.

Граница выводов

Сценарий вымышленный. Никакая система не проверялась для подготовки этого PDF. Указанные ниже состояния демонстрируют структуру записи, а не фактические результаты или опыт исполнителя.

> **Что должно быть в реальном отчёте**
>
> Согласованные объекты, время и версия, разрешённые действия, фактическое покрытие, ограничения и ответственные. Доказательства передаются отдельно от публичного образца.

DEMO-01
Право на скачивание документа

Учебная иллюстрация того, как отделить наблюдение, влияние и рекомендацию.

Ожидаемое правило	Пользователь организации А получает документы А и не получает документы Б.
Условие примера	Две искусственные учётные записи и два документа с учебными маркерами.
Вымышленное наблюдение	Список ограничен правильно, но отдельная выдача файла не использует то же правило принадлежности.
Статус	Демонстрационная находка. Не подтверждена на реальном объекте.

Как выглядело бы доказательство

В рабочей карточке указывают версию, среду, роль, учебный объект, ожидаемый результат и фактический ответ. Секреты и сведения настоящих клиентов не включают без необходимости. В этом образце доказательств реальной уязвимости нет.

Возможное влияние в учебной модели

Нарушение границы организаций могло бы раскрыть документ ненадлежащему участнику. Объём и последствия требуют отдельного подтверждения. По одному учебному объекту нельзя утверждать массовую утечку.

Направление исправления

Проверять принадлежность и разрешение на серверной операции выдачи. Сопоставить связанные пути: просмотр, скачивание и экспорт. Скрытие ссылки в интерфейсе не является достаточным критерием.

> **Вопрос владельцу процесса**
>
> Какие роли действительно вправе получать документ и меняется ли право после закрытия заявки? Это бизнес-правило нужно согласовать до проверки реализации.

Исправление должно иметь доказательство

Шаг	Ответственный в учебной модели	Проверяемый результат
Уточнить правило	Владелец продукта	Описаны роли, организации и разрешённые действия.
Подготовить изменение	Команда разработки	Сервер применяет правило на значимых путях выдачи.
Проверить регрессию	Тестирование	Свой документ доступен, чужой недоступен; законный экспорт работает.
Подтвердить внедрение	Эксплуатация	В нужной среде развёрнута проверенная версия.
Повторить проверку	Согласованный проверяющий	Зафиксированы среда, дата и результат исходного критерия.

Статусы не следует смешивать

Подготовленный патч, внедрённое изменение и проверенное устранение представляют разные этапы. Временное ограничение риска не считается устранением причины. Принятый остаточный риск требует владельца и условия пересмотра.

Ограничения повторной проверки

Повторный тест подтверждает согласованный сценарий в указанной версии. Он не является бессрочной гарантией и не оценивает автоматически новые функции, появившиеся после исходной проверки.

Методический ориентир

Для объяснения контекстного приоритета используется CISA SSVC. Источник не подтверждает учебную находку и не задаёт срок её исправления.

CISA SSVC Guide

> **Следующий шаг**
>
> Согласовать собственный контур, критерии результата и формат отчёта. Рабочие доказательства передаются через защищённый канал, а не публикуются вместо этого образца.