

Чек-лист внедрения ГОСТ Р 57580

Справочный и классификационный слой поверх модуля СУОН плюс показатели отчётности 716-П — модуль платформы «Ланселот». Вопросы ниже заданы от правил, которые уже заложены в продукте, а не от общих соображений о внедрении.

1. Что нужно решить до старта

- Кто администрирует справочники ИКА — модуль поставляется с двумя ролями, которым по умолчанию выданы права на чтение, запись, добавление и удаление всех четырёх справочников (operIka3, operIka4, operIka6, operIka8): «ИТ-менеджер» (managerIt) и «ИТ риск-менеджер» (riskManagerIt).
- Источник данных для справочника ИКА8 — в актуальном состоянии он заполняется классами конфиденциальности информации (Ограниченный / Конфиденциальный / Внутренний / Публичный) из импорта SimpleOne, а не исходной триадой значений «объекты информатизации / субъекты доступа / каналы передачи». Стоит заранее решить, какой состав значений актуален для вашей организации.
- Кто вводит показатели 716-П — все три показателя (716П1_121_21, _22, _23) помечены как вводимые вручную: расчётного механизма в модуле нет, значения заносит ответственный сотрудник через форму ввода фактов.
- Период и форма отчёта — показатели выгружаются в отчёт по форме 0409106; стоит заранее определить, кто готовит и проверяет выгрузку на вашей стороне.

2. Какие роли завести

Для работы со справочниками ИКА достаточно двух ролей, для которых права уже выданы миграцией продукта:

- ИТ-менеджер (managerIt) — чтение, запись, добавление и удаление элементов всех четырёх справочников ИКА; на карточке объекта поле «Классификация по системным уровням» обязательно для ИТ-продуктов, поле «Классификация сервисов поставщика облачных услуг» — для облачных решений.
- ИТ риск-менеджер (riskManagerIt) — тот же состав прав на справочники ИКА, что и у ИТ-менеджера.
- Отдельного права на саму вкладку «ИКА» карточки объекта в продукте нет: видимость вкладки не ограничена, а право на запись определяется правом на раздел «Описание» карточки.

3. Какие справочники подготовить

- Классификация по системным уровням (ИКА3) — пять значений: уровень аппаратного обеспечения, сетевого оборудования, сетевых приложений и сервисов, серверных компонентов виртуализации и инфраструктурных сервисов, операционных систем и СУБД.

- Классификация в контексте отсутствия уязвимостей (ИКА4) — три значения: ПО с доступом из интернета, ПО для установки у клиентов организации, иное.
- Классификация сервисов поставщика облачных услуг (ИКА6) — три значения: SaaS, PaaS, IaaS.
- Классификация в зависимости от класса обрабатываемой информации (ИКА8) — четыре класса конфиденциальности: Ограниченный, Конфиденциальный, Внутренний, Публичный, с полем приоритета для выбора самого строгого класса при загрузке из SimpleOne.
- Пороги показателей 716-П — для 716П1_121_21 и 716П1_121_22 сигнальное значение должно быть не менее 0,9, а контрольное — не менее 0,85; для всех трёх показателей контрольное значение не должно превышать сигнальное.

Модуль собирает, контролирует и подготавливает эти данные к отчёту; расчётного механизма, реализующего методику оценки соответствия по ГОСТ Р 57580.2-2018, в нём нет — показатели соответствия вводятся вручную.

ГОСТ Р 57580 — справочный и классификационный слой поверх модуля СУОН, платформа «Ланселот».
ООО «Ланселот-ИТ», РФ, г. Москва, ул. Профсоюзная 45.