

Чек-лист внедрения

Ланселот ПНИИИМР: Инциденты и риски

О файле. Пункты собраны из реальных параметров конфигурации продукта — того, что до запуска запрашивает db.properties, планировщик задач и модуль безопасности. Это не общий чек-лист внедрения ПО, а список решений и данных, которые нужны именно этому продукту, чтобы стартовать с рабочими ролями, уведомлениями и импортом.

1. Роли и права доступа

- Распределить сотрудников по ролям модуля безопасности. В продукте их 19: Риск-менеджер, Риск-эксперт, Риск-координатор, Риск-валидатор, Риск-администратор, Менеджер риска ИБ, Менеджер риска ИТ, Сотрудник СВК, Аудитор, Аудитор администрирования, Администратор, Системный администратор, ИБ-администратор, Администратор представлений, Пользователь представлений, Сотрудник банка, Комментатор и служебные роли автозагрузки.
- Роли securityAdmin, presentationAdmin и presentationUser создаются автоматически при первом старте — отдельно заводить их не нужно, но пароль администратора безопасности нужно сменить сразу после запуска.
- Права роли назначаются по объектам семи типов: справочник, действие, отчёт, маршрут статусов события, раздел события, категория события, раздел регуляторного риска. Решить заранее, какая роль видит какой раздел и какой отчёт — до раздачи доступа, а не после первого инцидента с правами.

2. Маршруты согласования

- Событие РР проходит маршрут из 24 статусов (от «Предсобытие» до «Закрето»), регуляторный риск — маршрут из 16 статусов. Проверить с бизнес-заказчиком, какие из статусов используются у вас, а какие можно скрыть в представлении списка.
- Для каждого статуса маршрута определить роль, которой доступен переход: часть переходов (например, «Предсобытие» → «Первичная валидация») в базовой поставке закрыта одной ролью — риск-координатором.
- Решить, какие подразделения используют признаки «ИТ-категория» и «ИБ-категория» у регуляторного риска — они меняют маршрут согласования записи.

3. Напоминания по срокам

- Задача напоминаний о сроках нахождения записи в статусе включается параметром scheduled.task.time (расписание cron) — без него уведомления «Взять в работу» и «Передать дальше» не отправляются вовсе.
- Пороги задаются в отдельном yaml-файле по параметру alertsubject.path: для каждой пары роль/статус указываются три порога — firstAlert, redAlert, deadAlert — и признак checkDepartment. Подготовить этот список по своим регламентным срокам до запуска: пустой файл — молчащая задача.
- Уведомления уходят двумя каналами — внутренним сообщением в колокольчике шапки (опрос раз в 5 секунд) и почтой; SMTP-сервер должен быть указан в db.properties.

4. Источники данных: почта, оргструктура, проводки

- Регистрация событий РР письмом: параметры почтового ящика bks.mail.risk.*; задача читает ящик раз в минуту и создаёт предсобытия сразу в статусе «Первичная валидация». Нужен отдельный ИМАР-ящик, выделенный под приём таких писем.
- Импорт оргструктуры из почтового архива — расписание import.structure.email.schedule (в базовой поставке — по будням в 8:00), источник — параметры import.structure.email.*. Обновляет подразделения, должности и сотрудников.

- Импорт проводок АБС — тот же механизм почтового архива, свои параметры источника. Решить, какая система выгружает проводки и с какой периодичностью.
- Помимо почты, продукт принимает импорт из файла (xlsx/csv/xlsb), базы данных и Active Directory — десять типов данных из четырёх источников; выбрать нужные на этапе настройки, а не включать все сразу.

5. Контрольные показатели и справочники

- 13 предзаполненных констант контрольных показателей Банка (kpr_constants) поставляются с кодами, но без итоговых значений — заполнить их значениями вашей организации до первого расчёта контрольных показателей.
- 21 редактируемый справочник и пять справочников качественной оценки событий РР (плюс два рейтинга) — согласовать состав значений с профильными подразделениями до переноса исторических данных.
- Классификаторы и измерения (раздел «Настройка измерений») задать до того, как в системе появятся первые рабочие записи: смена классификации на потоке данных дороже, чем настройка заранее.

6. Аутентификация и внешние системы

- Способ входа задаётся параметром authentication.type: локальная база (BCrypt), LDAP/Active Directory или Kerberos (файл keytab). Решить заранее, каким способом входят пользователи, — переключение меняет форму входа для всех.
- Интерактивный отчёт использует внешний BI-сервер (Pentaho) — раздел появляется в навигаторе, только если задан адрес сервера; без него доступны только встроенные Excel-выгрузки списков и типовые формы отчётности.
- Файловое хранилище MinIO — необязательный компонент; без него файлы хранятся в файловой системе сервера приложений.

7. Платформа и развёртывание

- Целевая среда: Java 8, Apache Tomcat 8.5, PostgreSQL; поставка — war-архив (bootWar) и шаблоны context.xml.template и db.properties.template.
- Действующие параметры подключения, аутентификации, почты и импорта читаются из файла db.properties в каталоге config.path — заполнить его по шаблону до первого запуска, а не полагаться на значения по умолчанию из application.properties.
- При старте приложение само применяет миграции Liquibase к базе данных — убедиться, что учётная запись подключения имеет права на изменение схемы перед первым запуском.

Список закрывает параметры, известные из конфигурации продукта. Регламентные сроки, состав ролей у ваших сотрудников и значения справочников — решения вашей организации, их вносит внедренческая команда на старте проекта.