Чек-лист: 43 проверки перед разбором события ПНИИИМР

Составлен по правилам, которые заложены в самом продукте «ПНИИИМР Ланселот: противодействие неправомерному использованию инсайдерской информации и манипулированию рынком». У каждой строки указано, откуда правило взято: файл и строки исходного кода либо норма права. Ничего не додумано.

> Как пользоваться. Пройдите разделы 1-7 по своему порядку рассмотрения обращений о возможном нарушении: если пункт у вас не описан внутренним документом, это дыра в правилах внутреннего контроля, а не в программе. Разделы 8 и 9 закрываете вы сами: продукт эти задачи не решает, и заявлять обратное мы не будем. Соответствие требованиям закона оценивает сама организация и её ответственное должностное лицо; программа даёт инструменты и оставляет доказательство выполнения.

1. Маршрут события: проходит ли обращение полный триаж

- [ ] Сообщение о возможном нарушении регистрируется как «Предсобытие» и переходит только в «Первичную валидацию»: прямого пути в согласование руководителю нет — переход отключён в самой статусной модели.
  источник: RiskStatus.java:42-43
- [ ] После первичной валидации предусмотрен запрос информации у инициатора и возврат по кругу: «Запрос информации у инициатора» → «Информация по запросу предоставлена» → «Первичная валидация».
  источник: RiskStatus.java:43-51
- [ ] Квалификация даёт ровно две развилки: «Закрыто. Не РР.» либо «Анализ: Оценка уровня риска» → «Анализ: Причины возникновения» → «Закрыто».
  источник: RiskStatus.java:43-51
- [ ] Проверьте, что ваш внутренний порядок описывает все 24 статуса события регуляторного риска и 30 переходов между ними, а не только «открыто/закрыто».
  источник: RiskStatus.java:15-38, 42-80
- [ ] Комментарий при переходе. В 24 переходах из 30 открывается диалог ввода комментария; триажный участок его не требует. Решите, где комментарий обязателен по вашим правилам, а где достаточно факта перехода.
  источник: RiskStatus.java:52-81

2. Ветвление и разделение обязанностей

- [ ] После верификации маршрут расходится на три независимые ветви — СПНП, менеджер риска ИБ, менеджер риска ИТ; согласующий одной ветви не согласует за другую.
  источник: RiskStatus.java:53-58, 59-69
- [ ] Финальное согласование выполняет эксперт: «Согласовать СПНП» → «Передано на согласование риск эксперту», далее закрытие, черновик или возврат СПНП.
  источник: RiskStatus.java:70-75
- [ ] Возврат по маршруту предусмотрен явными статусами «Возврат руководителю» и «Возврат СПНП» — проверьте, что в вашем порядке они описаны как штатные, а не как исключение.
  источник: RiskStatus.java:61-63, 72-75

- [ ] Закрытое событие переоткрывается («Закрыто» → «Переоткрыто»), и переоткрытие тоже должно быть описано в правилах.
  источник: RiskStatus.java:76-80

3. Роли и обязательные поля

- [ ] Состав обязательных полей вкладки «Описание» зависит от роли: для сотрудника (координатора риска) и руководителя обязательны 9 полей, для сотрудника СПНП — только статус. Сверьте это со своим порядком заполнения карточки.
  источник: RequiredModel.java:18-24, 41-54
- [ ] Если у работника несколько ролей, карточка собирается по одной «главной» — приоритет жёстко задан в коде. Убедитесь, что совмещение ролей у вас не приводит к неожиданному составу обязательных полей.
  источник: IncidentViewModel.java:350-400
- [ ] У сотрудника с единственной ролью координатора реестр предсобытий открывается в урезанном представлении. Проверьте, что это соответствует вашему разграничению ввода и последующей обработки.
  источник: NavigatorList.java:294-318
- [ ] Роли продукта: сотрудник СПНП, эксперт ПНИИИМР, менеджер риска ИБ, менеджер риска ИТ, аудитор, сотрудник СВК, руководитель, сотрудник, комментатор. Сопоставьте их со своими должностями до демонстрации.
  источник: RoleType.java:5-15

4. Разграничение доступа к материалам события

- [ ] Доступ выдаётся не «на экран», а на типизированный объект: справочник, действие, отчёт, статусная модель, раздел карточки, категория, раздел риска — у каждого свой набор допустимых действий.
  источник: Types.java:42-87
- [ ] Шесть базовых действий: READ, WRITE, ADD, DELETE, EXECUTE, FILTER. Действие FILTER ограничивает не объекты, а набор видимых строк.
  источник: Action.java:11-16; security/web/component/filter/
- [ ] Карточка события состоит из 12 разделов, и каждый раздел — самостоятельный объект безопасности. Определите, какие разделы кому видны.
  источник: RiskSection.java:15-26, 44-46
- [ ] Вложения с признаком «Ограниченный доступ» недоступны на скачивание и удаление без отдельного права manageSecretFiles.
  источник: Actions.java:34, 67
- [ ] Узел меню, на который нет права, не строится вообще — пользователь его не видит.
  источник: NavigatorList.java:765-773

5. Сроки, оповещения и «зависшие» события

- [ ] Контроль сроков двухпороговый: «жёлтый» и «критический» диапазоны считаются от даты последнего изменения. Пороги задаются в минутах.
  источник: ScheduledNotificationService.java:86-121

- [ ] Пороговые значения лежат во ВНЕШНЕМ YAML-файле, которого нет в поставке. Матрицу «роль → статус → пороги» заполняет ваша организация — заложите это в план работ.
  источник: AlertSettings.java:12 (alertsubject.path)

- [ ] Каналы оповещения ведут себя по-разному: в систему пишется отдельное сообщение на каждое просроченное событие, по почте уходит одно письмо со списком.
  источник: ScheduledNotificationService.java:202-253; templates.stg:10-17

- [ ] Есть отдельное предупреждение о разрыве маршрута: «Инцидент останется без рассмотрения. Инцидент в статусе … не доступен ни одному из пользователей системы». Проверьте, кто у вас на него реагирует.
  источник: templates.stg:8

- [ ] Адрес доставки берётся из служебного адреса работника в оргструктуре — актуальность этого реквизита критична для оповещений.
  источник: ScheduledNotificationService.java:186, 215, 253

6. Источники событий и импорт

- [ ] Автосоздание события из письма работает раз в минуту: система читает непрочитанные письма по IMAP, склеивает тему и тело в описание, определяет отправителя и создаёт событие в статусе «Первичная валидация».
  источник: RiskEmailSettings.java:48-88; RiskMailImporter.java:45-55

- [ ] Отправитель сопоставляется с работником по адресу электронной почты — справочник сотрудников должен быть актуален.
  источник: RiskMailImporter.java:69-73

- [ ] Ошибка обработки одного письма не прерывает цикл: решите, кто и как отслеживает необработанные сообщения.
  источник: RiskEmailSettings.java:48-88

- [ ] Источники импорта данных: файлы, внешняя база данных, Active Directory, почта. Сделок и торговых данных среди них нет.
  источник: SourceType.java:4-7; ActiveDirectorySource.java; DataSourceRowsReader.java

7. Реестр, отчётность и доказательство выполнения

- [ ] Реестр событий и «Предсобытия» — одно представление с противоположными фильтрами по статусу. Проверьте, что ваши регламентные выгрузки берут нужный.
  источник: NavigatorList.java:280, 310

- [ ] Табличное представление реестра содержит 26 колонок, включая признак «Событие является Регуляторным риском в области ПНИИИМР (ДА/НЕТ)».
  источник: cfgview_PresentationItem.csv:1-27

- [ ] Период отчёта — полузакрытый интервал: события на дату «по» в выборку не входят. Это прямо предупреждается в интерфейсе; учтите при сверке цифр.
  источник: incidents_report.zul:60, 95

- [ ] Плановая и фактическая даты выполнения мероприятия не могут быть раньше даты реализации события — контроль встроен.
  источник: zk-label_ru.properties:1047-1048

- [ ] Форма 0409106 — отчётность по операционному риску целиком, а не отчётность по ПНИИИМР. Отдельной регуляторной формы по инсайдерской информации в продукте нет, и её не должно быть в вашем плане.
  источник: web/report/incidents/report0409106/

8. Что закрываете вы, а не продукт

- [ ] Список инсайдеров и уведомление лиц о включении в него — сущности отсутствуют. Нужен отдельный реестр или ведение силами корпоративного секретаря.
  источник: требование: 224-ФЗ, ст. 9
- [ ] Список наблюдения и стоп-лист — сущностей нет, операцию продукт заблокировать не может.
  источник: требование: 23-МР, п. 1.1.13, п. 2.2.15
- [ ] Сбор сведений о совершённых операциях инсайдеров и мониторинг сделок — торговых данных продукт не получает и детектирующих алгоритмов не содержит.
  источник: требование: 224-ФЗ, ст. 10, ст. 12
- [ ] Раскрытие инсайдерской информации — механизмов публикации нет.
  источник: требование: 224-ФЗ, ст. 8
- [ ] Обучение работников и подтверждение ознакомления — модуля обучения нет.
  источник: требование: 5222-У, п. 1; 23-МР, пп. 1.1.8, 1.1.14
- [ ] Годовой пересмотр правил внутреннего контроля — версионирования внутренних документов в продукте нет.
  источник: требование: 5222-У, п. 1
- [ ] Физические меры защиты — вне контура любого программного обеспечения.
  источник: требование: 23-МР, пп. 2.2.7-2.2.10

9. Что нужно заполнить своими данными до запуска

- [ ] Справочник ссылок на нормативные документы поставляется пустым: перечень норм ПНИИИМР вносит ваша организация.
  источник: documents_links
- [ ] Матрица порогов регламентных оповещений задаётся внешним YAML-файлом, которого в поставке нет.
  источник: alertsubject.path
- [ ] Содержательных анкет по ПНИИИМР в поставке нет — есть конструктор анкет из 7 типов полей.
  источник: SurveyFieldType.java:8-14
- [ ] Оргструктура и справочник работников со служебными адресами — без них не работают ни сопоставление отправителя, ни оповещения.
  источник: ImportType.java:16-41

Оговорка. Продукт предоставляет инструменты, которыми организация исполняет процедуры своих правил внутреннего контроля. Оценка достаточности этих процедур и их соответствия требованиям Банка России относится к компетенции самой организации и её ответственного должностного лица. Материал носит информационный характер и не является публичной офертой или юридической консультацией. Всего пунктов в чек-листе: 43.