**Регламент диагностики и восстановления: 1С, SAP FI/MM, ЭДО, CI/CD, Kubernetes/Docker, Почтовые сервисы**

*Версия 1.0*

## 1. 1С / Бухгалтерский учет

**Назначение.** Документ устанавливает порядок выявления причин сбоев и восстановления работоспособности прикладных решений на платформе 1С:Предприятие 8.x. Цель состоит в минимизации простоя, сохранении целостности данных и обеспечении корректного обмена с внешними системами.

**Область применения.** Материал применяется к серверным кластерам 1С, тонким и толстым клиентам, серверам баз данных MS SQL и PostgreSQL, а также к интеграциям с системами электронного документооборота и смежными учетными системами.

**Признаки и возможные причины.** Не запускается клиент 1С; ошибки подключения к серверу или СУБД; зависания интерфейса и заметное замедление операций; ошибки регистров и расхождения в отчетах; прекращение формирования или отправки регламентированной отчетности; прерывание обменов с внешними сервисами. Типичные причины: недоступность сервера СУБД; дефицит CPU/RAM/диска; ошибки конфигурации кластера; конфликт версий платформы и конфигураций; повреждение ИБ из‑за некорректного завершения сеансов.

**Порядок проверки.** 1) Подтвердить сетевую доступность сервера СУБД: ping <db\_host>, telnet <db\_host> 1433|5432. 2) Проверить состояние служб 1С: systemctl status srv1cv83 (Linux) или оснастка «Службы» (Windows). 3) Оценить свободное место: df -h (Linux) или Get-Volume (Windows). 4) Изучить журнал регистрации 1С и журналы СУБД (errorlog, postgresql.log). 5) Контролировать подключения и активность сеансов в консоли администрирования кластера 1С.

**Порядок восстановления.** 1) Корректно завершить активные пользовательские сеансы. 2) Перезапустить службы сервера 1С и экземпляра СУБД. 3) Выполнить тестирование и исправление ИБ штатными средствами; при признаках повреждения восстановить из последней успешной резервной копии. 4) Перепровести документы проблемного периода, обновить регистры и проверить корректность обменов и регламентных заданий.

**Профилактика.** Регулярные резервные копии с проверкой восстановления; централизованное обновление платформы и конфигураций; мониторинг CPU, RAM, диска и блокировок в СУБД; плановая проверка журналов на ошибки логической корректности и деградации производительности.

**Контроль.** Фиксировать результаты в журнале инцидентов: временные метки, характер ошибки, предпринятые действия, подтверждение восстановления работоспособности.

## 2. SAP FI/MM

**Назначение.** Определяет порядок диагностики и восстановления процессов финансового учета и материального менеджмента в SAP при операционных сбоях.

**Область применения.** Транзакции FI и MM, отчёты налогового учета (включая RFUMSV00), интерфейсы интеграции с внешними системами.

**Признаки и возможные причины.** Ошибки проводок в FI, MIRO или FB60; зависания при запуске отчетов; некорректные налоговые коды и ставки; отклонения в RFUMSV00; нестабильность интеграций по IDoc или RFC; неверные фильтры в ALV. Причины: некорректные мастер‑данные поставщиков и материалов; неверные налоговые ключи; закрытие периода; конфликтующие пользовательские фильтры и параметры отчетов; сетевые или авторизационные ограничения.

**Порядок проверки.** 1) Проверить доступность приложений и портов: ping <sap\_app>, telnet <sap\_app> 32xx. 2) Проанализировать ST22, SM21, SM37, SM13 и блокировки в SM12. 3) Пересмотреть параметры RFUMSV00 с учетом периода и отборов; очистить пользовательские фильтры в ALV; актуализировать мастер‑данные и налоговые коды; при необходимости открыть соответствующий период.

**Порядок восстановления.** Скорректировать параметры транзакций; выполнить повторное проведение документов; перезапустить фоновые задания; синхронизировать интеграции; привести варианты ALV к стандартизированным шаблонам; обновить кэш; сформировать повторный отчет и сверить результаты.

**Профилактика.** Утвердить регламент изменения мастер‑данных; контролировать параметры налогообложения и шаблоны отчетов; регулярно очищать блокировки и кэши; сопровождать интеграции мониторингом; валидировать периоды закрытия.

**Контроль.** В отчет включать использованные транзакции, номера документов, выполненные корректировки, перезапуски и результаты сверки.

## 3. Электронный документооборот (Диадок, Контур, СБИС)

**Назначение.** Порядок настройки, проверки и восстановления обмена электронными документами через операторов ЭДО, включая работу с электронными подписями.

**Область применения.** Встроенные модули ЭДО в 1С и отдельные клиентские приложения операторов.

**Признаки и возможные причины.** Документы не отправляются/не принимаются; статусы долго «в ожидании»; подпись отклоняется из‑за недействительного сертификата; форматы КНД не распознаются; транспортные ошибки. Причины: истекший сертификат; разрыв цепочки доверия; неверная привязка к учетной записи/токену; отсутствие закрытого ключа; устаревшие корневые сертификаты и плагины; сетевые ограничения.

**Порядок проверки.** 1) Проверить срок действия и цепочку доверия: certmgr.msc (Windows) или openssl x509 -in cert.cer -text -noout. 2) Валидировать привязку сертификата и наличие закрытого ключа на токене. 3) Подписать тестовый документ и сверить форматы КНД. 4) Проанализировать статусы у контрагентов. 5) Проверить сетевую доступность сервисов ЭДО и актуальность плагинов.

**Порядок восстановления.** Выпустить и установить новый сертификат с актуальными корневыми; перепривязать сертификат к учетной записи; повторно отправить документы и при необходимости инициировать повторную доставку; обновить клиент/плагин ЭДО; перезапустить рабочую станцию.

**Профилактика.** Календарь ротации сертификатов; резервные носители подписи; ежедневный контроль протоколов и статусов; актуальность корневых сертификатов и версий плагинов.

**Контроль.** Фиксировать ИНН контрагента, тип и номер документа, текущий статус, хэш протокола и исполнителя.

## 4. CI/CD и DevOps

**Назначение.** Стандартизированный порядок диагностики и восстановления конвейеров непрерывной интеграции и доставки ПО.

**Область применения.** Системы CI/CD (например, GitLab CI и Jenkins), взаимодействие с системами контроля версий, реестрами образов и инфраструктурным кодом.

**Признаки и возможные причины.** Пайплайны завершаются по тайм‑ауту или из‑за ошибок зависимостей; агенты не подхватывают задания; не проходит аутентификация к репозиторию или реестру; повреждены кэш/артефакты; дрейф зависимостей. Причины: сетевые и прокси‑ограничения; неверные SSH‑ключи или токены; недостаточные временные/ресурсные лимиты.

**Порядок проверки.** 1) Проверить доступ к репозиторию: ssh -T git@<host>, git ls-remote. 2) Войти в реестр образов: docker login <registry>; проверить доступ: curl -I <url>. 3) Проанализировать логи агента и состояние очереди; проверить переменные окружения. 4) Перезапустить пайплайн без кэша; уточнить тайм‑ауты по стадиям.

**Порядок восстановления.** Пересоздать кэши и артефакты; зафиксировать версии зависимостей в lock‑файлах; настроить повторные попытки и увеличить тайм‑ауты на нестабильных шагах; актуализировать ключи и токены; обновить список доверенных хостов; задокументировать изменения.

**Профилактика.** Закрепление версий зависимостей; репликация реестра образов; SLO для пайплайнов; обязательные smoke‑тесты и security‑чеки; алертинг по падениям и долгим задачам.

**Контроль.** Фиксировать идентификатор коммита, номер пайплайна, список стадий, длительность, ответственных и ссылки на артефакты.

## 5. Kubernetes / Docker

**Назначение.** Диагностика и восстановление контейнерных приложений в средах Kubernetes и Docker.

**Область применения.** Рабочие кластеры, пространства имен, ingress‑контроллеры и реестры образов.

**Признаки и возможные причины.** Недоступность приложения; CrashLoopBackOff или ImagePullBackOff; трафик не проходит через Ingress/Service; повышенная задержка и рост ошибок. Причины: некорректные секреты для реестра; ошибки readiness/liveness; неверные ограничения ресурсов; сетевые политики и маршрутизация.

**Порядок проверки.** 1) kubectl get pods -n <ns> -o wide; kubectl describe pod <name> -n <ns>. 2) kubectl get events -n <ns>; kubectl logs <pod> -n <ns>. 3) Проверить secrets и configmaps: kubectl get secrets, kubectl get configmaps. 4) Проверить настройки ingress и service.

**Порядок восстановления.** Актуализировать секреты и imagePullSecrets; подтвердить доступ к реестру; скорректировать readiness/liveness; пересмотреть requests/limits; выполнить перекат релиза Helm с параметром --atomic; при необходимости откатиться до проверенной версии.

**Профилактика.** Регулярное сканирование образов; контроль дрейфа конфигураций; квоты ресурсов и горизонтальное авто‑масштабирование; мониторинг задержек и частоты ошибок; периодическая валидация ingress и сетевых политик.

**Контроль.** Фиксировать версию чарта и образа, перечень изменений, причину сбоя и подтверждение стабильной работы после исправления.

## 6. Outlook / Exchange / Почтовые сервисы

**Назначение.** Порядок устранения неполадок почтовых клиентов и серверной части инфраструктуры Exchange и SMTP.

**Область применения.** Рабочие станции с Outlook, а также почтовые серверы, шлюзы и политики безопасности.

**Признаки и возможные причины.** Почта не отправляется/не доставляется; клиент не подключается и зависает при синхронизации; письма попадают в карантин или спам. Причины: неверные учетные данные; поврежденный профиль клиента; некорректные политики шлюза безопасности; нарушения DMARC/SPF/DKIM; сетевые и квотные ограничения.

**Порядок проверки.** 1) Проверить доступность серверов: ping <mail\_host>, telnet <mail\_host> 25|443. 2) Пересоздать профиль клиента; проверить автоконфигурацию (Autodiscover, тест подключения). 3) Проанализировать карантин, транспортные правила и журналы SMTP.

**Порядок восстановления.** Очистить или пересоздать профиль; перезапустить клиентские службы; исправить записи SPF, DKIM и DMARC; актуализировать белые списки; увеличить квоту ящика или выполнить очистку; проверить отправку и доставку тестовых сообщений.

**Профилактика.** Мониторинг репутации домена и отчетов DMARC; регулярные обновления клиента и плагинов; требования к паролям и MFA; контроль корректности транспортных правил и антиспам‑политик.

**Контроль.** Указывать адреса отправителя и получателя, заголовки (Message-ID), время обработки, задействованное правило и итог доставки.

## Глоссарий терминов и определений

**Сертификат электронной подписи.** Набор ключевых данных пользователя (открытый и закрытый ключ), используемый для подписания электронных документов и проверки их подлинности.

**DMARC, SPF и DKIM.** Механизмы проверки подлинности и целостности почтовых сообщений и доменов, снижающие уровень спуфинга и фишинга.

**Runner или Agent.** Исполняющий компонент системы CI/CD, запускающий задания конвейера в соответствии с конфигурацией.

**CrashLoopBackOff.** Состояние контейнера в Kubernetes, при котором процесс многократно завершается с ошибкой вскоре после запуска.

**RFUMSV00.** Стандартный отчёт SAP для анализа и сверки данных по НДС за период.

**Журнал регистрации 1С.** Системный журнал платформы 1С, фиксирующий операции и ошибки; используется для диагностики производительности и целостности.