



Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Безопасность 1С: роли, доступ к зарплате и аудит действий

Группы доступа БСП, RLS на зарплатные данные и журнал регистрации — наша схема внедрения

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

Суть проблемы

Наводим порядок в доступе к 1С: персональные учётки вместо общего «Admin», права через группы доступа БСП, зарплатные данные под RLS и работающий журнал регистрации. Без этого инцидент — удалённая платёжка, правка накладной задним числом, утечка ведомости — не расследуется: в логах безликая общая учётка, а «скрытые» отчёты открываются консолью запросов.

Почему это важно бизнесу

- Утечка зарплатной ведомости внутри коллектива — конфликты, уход ключевых людей и претензии по 152-ФЗ о персональных данных
- Правки документов задним числом без журнала недоказуемы: недостача спишется на «пересорт», а не взыщется с виновного
- Учётка уволенного с полными правами — готовая точка входа для шифровальщика; простой бухгалтерии в отчётный период — от недели
- Без персональных логинов расследование невозможно в принципе: ни для суда, ни для страховой, ни для внутренних выводов

Ключевые параметры реализации

8.3.25

ветка платформы, на которую
выравниваем базы: актуальные
механизмы паролей, журнала и RLS
по докам 1С:Предприятие 8.3

12 симв.

минимальная длина пароля +
проверка сложности в «Настройках
входа» БСП, срок действия 90 дней
наш стандарт (БСП 3.1)

БСП 3.1

производительный вариант RLS:
шаблоны
«ДляОбъекта»/«ДляРегистра» и
ключи доступа вместо вложен...
по докам БСП «Управление доступом»

День

периодичность разделения
журнала регистрации (.lgf):
быстрее отбор и усечение при
архивировании
по докам ЖР 1С 8.3

24 мес

глубина архива выгрузок журнала
регистрации вне сервера — хватает
на разбор инцидента и провер...
наш стандарт

1 раз/кв

ревизия групп доступа и сверка
пользователей ИБ с кадровым
списком, результат фиксируем
актом
наш стандарт

Ролевая модель через группы доступа БСП

Что настраиваем

БП 3.0 / ЗУП 3.1 на сервере 1С:Предприятия; все пользователи ИБ, включая сервисные и обслуживающие учётки

Как мы это делаем

- 1 Инвентаризация пользователей ИБ: список в конфигураторе + справочник «Пользователи» и отчёт «Права доступа» БСП, сверка с кадрами; «сироты» и уволенные — немедленно...
- 2 Каждому сотруднику персональная учётка; в «Настройках входа» БСП: длина пароля 12, сложность, срок 90 дней; сервисным — запрет смены пароля и показа в списке выбора
- 3 Права назначаем только через профили групп доступа («Расчётчик», «Кадровик без доступа к зарплате», свои профили) — роли напрямую в конфигураторе не раздаём
- 4 «Полные права» оставляем одной выделенной админ-учётке; у остальных снимаем права «Интерактивное открытие внешних отчетов» и «Интерактивное открытие внешних обработ...

РЕЗУЛЬТАТ

Любое действие в базе привязано к конкретному человеку, права читаются отчётом «Права доступа» без раскопок в конфигураторе, а обновление конфигурации не ломает выданный доступ: профили БСП переживают апдейты, в отличие от ролей, розданных вручную.

КЛЮЧЕВОЙ НЮАНС

Смотрим в доке БСП раздел «Управление доступом»: поставляемые профили обновляются вместе с конфигурацией, поэтому кастомные права оформляем отдельными профилями, а не правкой типовых.



RLS: закрываем зарплатные данные на уровне записей

Что настраиваем

ЗУП 3.1 и зарплатный контур БП 3.0; виды доступа «Организации» и «Группы доступа физических лиц»

Как мы это делаем

- 1 Включаем «Ограничивать доступ на уровне записей» в Настройках пользователей и прав; вариант работы — производительный (шаблоны «ДляОбъекта»/«ДляРегистра»)
- 2 Раскладываем физлиц по справочнику «Группы доступа физических лиц»: руководство, свой отдел, прочие; профилям задаём разрешённые значения по видам доступа
- 3 Контролируем пересчёт ключей доступа регламентным заданием «Обновление доступа на уровне записей» — доступ раздаём только после его завершения
- 4 Прогон на копии: замер времени ключевых отчётов до/после и проверка под учёткой рядового бухгалтера через консоль запросов — чужие строки не возвращаются

РЕЗУЛЬТАТ

Ограничение работает на уровне запроса к СУБД: зарплату не достать ни универсальным отчётом, ни консолью запросов, ни внешней обработкой. Руководитель отдела видит начисления только своей группы физлиц, при этом отчёты не деградируют — ключи доступа считаются заранее, а не в каждом запросе...

КЛЮЧЕВОЙ НЮАНС

RLS-условие выполняется в каждом запросе: стандартный вариант (шаблон «ПоЗначениям») на больших таблицах даёт вложенные запросы, производительный переносит цену на запись. Вариант выбираем по замерам, не по ум...



Сквозной аудит: журнал регистрации, версии, даты запрета

Что настраиваем

Сервер 1С + СУБД; журнал регистрации платформы, подсистемы БСП «Версионирование объектов» и «Даты запрета изменения»

Как мы это делаем

- 1 Журнал регистрации: пишем все уровни событий, периодичность разделения «День»; на файловых базах каталог 1Cv8Log выносим с системного диска
- 2 Ежеквартально выгружаем журнал в XML из конфигуратора и усекаем с сохранением копии; архив храним 24 месяца вне сервера 1С
- 3 Включаем версионирование объектов для ведомостей, платёжек и справочника контрагентов: видно, кто и какой реквизит менял, с откатом на версию
- 4 Даты запрета изменения закрывают правки задним числом после сдачи периода; техжурнал logcfg.xml с событиями EXCP/CONN — для разбора аварий и подозрительных подклуче...

РЕЗУЛЬТАТ

По любому спорному документу восстанавливается цепочка: кто создал, кто и когда правил, какие значения были до изменения. Правка «задним числом» либо блокируется датой запрета, либо остаётся в журнале и версиях — разбор инцидента занимает часы, а не дни с банковской выпиской.

КЛЮЧЕВОЙ НЮАНС

Смена прав пользователей — сама по себе событие журнала: ставим на неё отдельный отбор. Формат .lgd (SQLite) не делится по периодам — держим последовательный .lgf (по умолчанию с 8.3.12) с разделением.



Подводные камни

✗ Общая учётка на отдел

Журнал пишет события, но субъект один на всех — расследование невозможно. Разносим по персональным учёткам, старую общую блокируем в тот же день

✗ Роли розданы мимо групп доступа

Назначенные напрямую роли не видны отчётам БСП и теряются при ревизии и обновлениях. Назначаем доступ только через профили групп доступа

✗ Спрятали кнопку вместо RLS

Пункт меню скрыт, но консоль запросов и внешняя обработка данные вернут. Закрываем RLS и снимаем права интерактивного открытия внешних отчётов и обра...

✗ Самописный RLS вложенными запросами

Ручные условия на больших таблицах роняют отчёты в разы. Используем шаблоны БСП и производительный вариант с предрасчётом ключей доступа

✗ Журнал регистрации не чистят годами

Файл растёт до десятков ГБ, отбор виснет. Держим .lgf с периодичностью «День», раз в квартал выгружаем в XML и усекаем с сохранением копии

✗ Кластер серверов без пароля админа

Без пароля администратора кластера консоль открыта любому в сети. Ставим пароль, порты администрирования 1540 (ragent) и 1545 (RAS) — только с админ-...

✗ RLS включили сразу в продуктиве

Пересчёт ключей доступа и новые условия меняют время отчётов и записи. Сначала копия базы и замер до/после, включение — вне рабочего времени

✗ Забытые пользователи ИБ

Учётки фрилансеров и уволенных живут годами с полными правами. Ежеквартальная сверка списка пользователей ИБ с кадровыми приказами

Как правильно

МИНИМУМ

- Персональные учётки всем; общие «Admin»/«Бухгалтерия» заблокированы
- Пароли: длина 12, сложность, срок 90 дней через «Настройки входа» БСП
- Журнал регистрации: все уровни событий, отбор по зарплатным документам
- RDP к серверу 1С из интернета закрыт, вход только через VPN

НОРМАЛЬНО

- Права только через профили групп доступа, «Полные права» — одна учётка
- RLS на зарплату: «Группы доступа физлиц», производительный вариант БСП
- Ежеквартально: выгрузка журнала в архив + ревизия прав с актом
- Даты запрета изменения после закрытия каждого отчётного периода

ХОРОШО

- Версионирование объектов на ведомости, платёжки и контрагентов
- Техжурнал (EXCP/CONN) + разбор отказов аутентификации по журналу
- Пароль администратора кластера, профили безопасности для внешних обработок
- 2FA на терминальном шлюзе, ежеквартальный тест восстановления бэкапа



Чек-лист самопроверки

- | | |
|---|---|
| ☐ У каждого сотрудника персональная учётка 1С, а общие логины «Бухгалтерия»/«Admin» заблокированы? | ☐ Учётки уволенных блокируются в день увольнения, сверка с кадрами идёт раз в квартал? |
| ☐ «Полные права» есть только у одной выделенной админ-учётки, а не у половины отдела? | ☐ Пароль администратора кластера серверов 1С установлен, консоль администрирования доступна только с админ-хостов? |
| ☐ Зарплата закрыта RLS, а не скрытым пунктом меню — проверяли под учёткой бухгалтера через консоль запросов? | ☐ Даты запрета изменения установлены и передвигаются после сдачи отчётности? |
| ☐ Права интерактивного открытия внешних отчётов и внешних обработок сняты у обычных пользователей? | ☐ RDP к серверу 1С недоступен из интернета, вход только через VPN или шлюз с 2FA? |
| ☐ Журнал регистрации пишет все уровни событий и раз в квартал выгружается в архив вне сервера? | ☐ Есть свежая копия базы и подтверждённый тест восстановления за последние 3 месяца? |

Если хотя бы на два вопроса ответ «нет» или «не знаю» — тема требует внимания.



Как поможет ITFresh

ITFresh — ИТ-аутсорсинг для юридических лиц до 50 рабочих мест в Москве и области. 15+ лет практики, собственная инфраструктура в дата-центре МТС (8 серверов Dell Xeon Platinum).

- Аудит доступа за 1 день: пользователи ИБ, роли, RLS, журнал, периметр — отчёт с приоритетами для руководителя
- Внедрение ролевой модели и RLS на зарплату без остановки бухгалтерии: 3-7 рабочих дней, тесты на копии базы
- Настройка журнала регистрации, версионирования и дат запрета + регламент ежеквартальной выгрузки в архив
- Закрытие периметра: VPN/шлюз с 2FA вместо открытого RDP, пароль кластера, бэкапы с тестом восстановления
- Сопровождение: ежеквартальная ревизия прав и сверка учёток 1С с кадровыми приказами

15+

лет в ИТ-поддержке

50

рабочих мест — наш профиль

МТС

дата-центр, Москва



КОНТАКТЫ

Обсудить вашу задачу

Сайт **itfresh.ru**

Телефон **+7 903 729-62-41**

Telegram **@ITfresh_Boss**

Бесплатно посмотрим вашу инфраструктуру по этому чек-листу и скажем, где тонко — без обязательств.



itfresh.ru



Техническая база

- 01** Руководство администратора: журнал регистрации, форматы .lgd/.lgf (its.1c.ru — 8.3)
- 02** БСП: подсистема «Управление доступом», производительный вариант RLS (its.1c.ru — 3.1)
- 03** БСП: «Версионирование объектов» и «Даты запрета изменения» (its.1c.ru — 3.1)
- 04** Руководство администратора: кластер серверов, rac/ras, профили безопасности (its.1c.ru — 8.3)
- 05** ЗУП 3.1: настройки пользователей и прав, группы доступа физлиц (its.1c.ru — 3.1)
- 06** Шаблон ITfresh «Аудит прав и журнала регистрации 1С» (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.

