**АУДИТ РЕАЛИЗАЦИИ СИСТЕМЫ УПРАВЛЕНИЯ ПЕРСОНАЛОМ (SAP/HR)**

**ПОЛЕВОЙ АУДИТ: ПРОГРАММА РАБОТЫ**

| **Nr** | **Процесс** | **Неотъемлемый риск (до осуществления контроля)** | **Оценка риска** | **Компенсирующие средства контроля для снижения риска/ характеристики**  **(ожидаемые)** | **Тестирование дизайна системы** | **Адекватность контроля** | **Тестирование реализации** | **Перекрестная ссылка**  **Результативность контроля** | **Вывод** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | Конфиденциальность  **DS5 Обеспечение безопасности систем** | Не исключен доступ к особо важной и конфиденциальной информации тем лицам, которые не должны иметь к ней доступ.  Автоматизированные деловые транзакции и информационный обмен не вызывают доверия. | Высокий  Высокий | * *Определен и поддерживается план обеспечения информационной безопасности.* * *Определен, внедрен и функционирует процесс управления идентификацией.* * *Отслеживаются потенциальные и фактические инциденты, связанные с безопасностью.* * *Права доступа и привилегии пользователей системы периодически пересматриваются и подтверждаются.* * *Поддерживается полнота, точность, действительность и доступность данных, хранящихся в системе.* * *Внедряются и поддерживаются технические и процедурные средства контроля для защиты информационных потоков во всех сетях.* * *Периодически проводятся проверки уязвимости данных.* | Установление наличия плана обеспечения информационной безопасности.  Анализ планов и определение того, содержат ли они описание компенсирующих средств контроля.  Установление того, содержится ли описание процедур, относящихся к целостности информационных потоков и данных. Анализ этих процедур в сравнении с компенсирующими средствами контроля. |  | * Установление количества инцидентов в связи с нарушениями физической безопасности или сбоями, а также количества случаев несанкционированного доступа к компьютерным устройствам. * Проведение теста на проникновение с целью тестирования компенсирующих средств контроля, предназначенных для предотвращения утраты конфиденциальной информации. * Проведение интервью с ключевыми специалистами, отвечающими за общие системы контроля, относящиеся к безопасности. * Проведение интервью с основными пользователями системы. |  |  |