Лекция 3

# **Направления ИТ аудита (**Что может входить в ИТ аудит?)

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Название раздела** | **Что получит бизнес** |
| 1 | **«Аудит IT инфраструктуры»** | Понимание состояния ИТ инфраструктуры с ее рисками,  узкими местами |
| 2 | **«Аудит IT персонала»** | Понимание состояния текущего ИТ персонала. Понимание  текущих рисков в существующем составе в штатном расписании |
| 3 | **«Опрос ключевых бизнес пользователей»** | Понимание текущей удовлетворенности бизнес пользователей.  Понимание возможных текущих потерь и  потребностей (возможные выгоды) бизнеса из-за ИТ. |
| 4 | **Аудит ИТ стратегии** | Оценка соответствия стратегическим целям Бизнеса. В результате данного аудита ТОП менеджмент и акционеры получат объективную и независимую оценку ИТ процессов и рекомендации по их оптимизации для выравнивания тактических планов ИТ со стратегическими и приведения ИТ стратегии в соответствие со стратегией бизнеса. |
| 5 | **«Анализ IT затрат»** | Оценка прозрачности ИТ затрат и их эффективности.  Рекомендации по процессам бюджетирования,  обоснованности ИТ расходов и получения максимальной  отдачи в интересах бизнеса.  Ответы на вопросы:   * Сколько компания тратит на IT? * Насколько это адекватно? * Сравнение с данными по отрасли (Benchmarking) |
| 6 | **«Анализ работы с контрагентами»** | Позволит получить представления по текущей  работе с внешними поставщиками, провайдерами.  Насколько эта работа выстроена оптимально и нет ли  здесь текущих или возможных потерь денег |
| 7 | **«Аудит корпоративной информационной системы»** | Поможет оценить риски при управлении бизнесом, при  дальнейшем развитии бизнеса, соответствие  современным требованиям |
| 8 | **«Краткий аудит IT процессов»** | Существующие риски в организационной модели  текущей IT службы. Какие потери могут возникнуть в  будущем из-за этого |
| 9 | **Аудит SLA**  **(Service Level Agreemen)** формальный договор между заказчиком услуги и её поставщиком, содержащий описание услуги, права и обязанности сторон и, самое главное, согласованный уровень качества предоставления данной | В результате данного аудита ТОП менеджмент и акционеры  получат объективную и независимую оценку ИТ процессов  связанных с предоставлением ИТ услуг, анализ эффективности  сорсинга (привлечение внешних ресурсов)  (инсорсинг и аутсорсинг).  В результате будут  предложены пути повышения эффективности  предоставления ИТ услуг |
| 9.1 | **«Разработка каталога сервисов и SLA»** | Каталог сервисов. Необходим для выстраивания  работы службы, взаимоотношений между ИТ и бизнес  подраздлениями |
| 10 | **Оценка планов BCP и ITCP**  **(Business** **Continuity** **Plan** **- план обеспечения непрерывности, восстановления после кризисных ситуаций)**  **Disaster Recovery Plan (DRP) - план восстановления после катастрофы** | В результате данного аудита будет предоставлена оценка  жизнеспособности планов BCP/DRP и предоставлены  рекомендации для повышения «отказоустойчивости»  ключевых бизнес-процессов, зависимых от ИТ.  Будут предложены пути повышения эффективности планов ITCP |
| 11 | **Информационная безопасность** | Оценка эффективности процессов Информационной  безопасности и/или их соответствия требованиям ISO 27001 |
| 12 | **Информационная безопасность** | Оценка процессов обработки и защиты ПДн требованиям  Законодательства в соответствии с 152-ФЗ и Приказ №21 ФСТЭК |
| 13 | **«Аудит ведущихся проектов»** | Понимание текущего состояния по ведущимся и прошедшим  IT проектам за период. Имелись ли потери, в каком размере |
| 14 | **«Аудит проектного управления в IT»** | Понимание существующих рисков в проектном управлении.  Какие потери могут возникнуть в будущем в ИТ проектах компании |
| 15 | **«Анализ рисков. Оценка управления ИТ рисками и/или бизнес-рисков, зависимых от ИТ.»** | Даст представление по всем рискам (в т.ч. и перечень  невыявленных), их сравнительную оценку, влияние,  вероятность реализации, краткое описание превентирующих  мероприятий |

**Что может быть результатом IT аудита?**

* Сводные отчет по текущему состоянию ИТ в компании
* План работы ИТ на 1-2-3 года
* Детальная проработка проектов по этому плану

**Аудит информационной безопасности** — системный процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности автоматизированной системы в соответствии с определёнными критериями и показателями безопасности.

**Аудит информационной безопасности** – проверка соответствия требованиям **ISO/IEC 27001** — международный стандарт по информационной безопасности, разработанный совместно Международной организацией по стандартизации и Международной электротехнической комиссией. Подготовлен к выпуску подкомитетом SC27 Объединенного технического комитета JTC 1. Стандарт содержит требования в области информационной безопасности для создания, развития и поддержания Системы менеджмента информационной безопасности (СМИБ).

**Информационная безопасность** — состояние сохранности информационных ресурсов и защищенности законных прав личности и общества в информационной сфере

**Стратегическая цель АИБ:** добиться максимальной отдачи от средств, инвестируемых в создание и обслуживание системы безопасности фирмы.

**Аудит позволяет**: оценить текущую безопасность; оценить и прогнозировать риски; управлять влиянием рисков ИБ на [бизнес-процессы](https://ru.wikipedia.org/wiki/%D0%91%D0%B8%D0%B7%D0%BD%D0%B5%D1%81-%D0%BF%D1%80%D0%BE%D1%86%D0%B5%D1%81%D1%81) фирмы, корректно и обоснованно подойти к вопросу обеспечения безопасности её информационных активов, стратегических планов развития, маркетинговых программ, финансовых и бухгалтерских ведомостей, содержимого корпоративных баз данных.