Лекции 1- 2

**АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

**Общие аспекты аудита информационной технологии**

**Аудит** – это периодическая, формальная проверка процесса или объекта.

**Аудит информационных систем и технологий** - системный процесс получения и оценки объективных данных о текущем состоянии информационных систем и технологий, действиях и событиях происходящих в них, устанавливающий и фиксирующий уровень их соответствия определенному критерию.

Показательным в этой связи является определение **аудита по глоссарию ITIL**: «**Аудит** - формальное обследование и проверка на предмет соблюдения какого-либо Стандарта или набора Руководящих документов или точности ведения Записей, или уровня достижения целевых показателей по Эффективности и Результативности. Аудит может проводиться внутренними или внешними службами».

Согласно очередному отчету MITRE, старое доброе переполнение буфера и в 2023 году сохраняет первое место среди самых опасных уязвимостей, попавших в перечень Common Weakness Enumeration. Собственно, вся первая тройка не меняется уже много лет, второе место плотно занимает XSS, третье — SQL injection. Зато на четвертое место с седьмого внезапно поднялась уязвимость класса CWE-416 — использование памяти после ее освобождения. <https://bugtraq.ru/rsn/archive/2023/06/01.html>





**DLP** (Data Loss Prevention) — специализированное программное обеспечение, предназначенное для защиты компании от утечек информации

**Форензик** — комплекс услуг, которые направлены на выявление корпоративного мошенничества, неправомерных действий сотрудников и коррупции в компании

# **ИТ аудит нужен, если:**

* Вы просто хотите оценить текущее состояние информационной системы.
* Вы не понимаете, зачем Вы тратите столько денег на IT и можно ли безболезненно сократить эти затраты;
* необходимо найти, где сейчас Вы теряете деньги из-за  некачественной работы IT специалистов;
* необходимо оценить критичность IT сервисов для Вашего бизнеса;
* Вы хотите узнать, ЧТО не так в Вашей информационной системе;

**В ИТ-аудит решает вопросы**:

* какие IT-инновации нужны предприятиям?
* как сохранить эффективность функционала IT при сокращенном бюджете и влиянии санкций?
* что внедрить сегодня для снижения затрат завтра?
* обеспечение комплексной безопасности информационной инфраструктуры.

# **Что Вы получите?**

* Четкую картину реального положения IT в Вашей компании;
* Понимание, где и сколько, если это возможно, Вы можете сократить на IT;
* Знание, где Вы теряете или можете потерять деньги;
* Представление о том, как Вы можете улучшить свой бизнес с помощью информационных технологий;
* Полный отчет с нашими рекомендациями по улучшению текущего положения.

## **Стандарты и практики, применяемые в ходе проведения IT аудита**



Эффективность работы информационных систем оценивается в рамках оценки эффективности ИТ процессов и соответствие этих процессов стандартам и лучшим практикам:

* **CobiT** - (сокращение от Control Objectives for Information and Related Technologies («Задачи управления для информационных и смежных технологий») — представляет собой пакет открытых документов, около 40 международных и национальных стандартов и руководств в области управления IT, аудита и IT-безопасности. Определение из ITIL: (Постоянное улучшение услуг) Control Objectives for Information and related Technology (COBIT) является руководством и Лучшей практикой по управлению ИТ- процессами. COBIT опубликован IT Governance Institute. Более подробно смотри также http://www.isaca.org/
* **IT Governance -** структура управления, входящая неотъемлемой составной частью в структуру управления предприятием и гарантирующая, что ИТ служит целям бизнеса, а не своим собственным, и что связанные с ИТ риски надлежащим образом
* **Val IT -** система управления ИТ-технологиями;
* **ITIL** - IT Infrastructure Library — библиотека инфраструктуры информационных технологий) — библиотека, описывающая лучшие из применяемых на практике способов организации работы подразделений или компаний, занимающихся предоставлением услуг в области информационных технологий
* **ITSM -** (IT Service Management, управление ИТ-услугами) — подход к управлению и организации ИТ-услуг, направленный на удовлетворение потребностей бизнеса.
* **Prince2 (**PRojects IN Controlled Environments 2) - структурированный метод управления проектами, одобренный правительством Великобритании в качестве стандарта управления проектами в социальной сфере. Методология **PRINCE2** включает в себя подходы к менеджменту, контролю и организации проектов.

**Базовые принципы ИТ-аудита**

* + - независимость и объективность
    - профессиональная компетентность
    - конфиденциальность

**Критерии ценности аудиторского заключения**

* + - достоверность: выводы основаны на фактах, которые могут быть повторно проверены, а так же на изучении достаточного количества информации.
    - актуальность: при изучении основной акцент делается на проблемах и рисках, которые уже реализуются или с высокой вероятностью могут быть реализованы в краткосрочной перспективе.
    - ясность: информация излагается в структурированном виде — от общих выводов в бизнес-терминах для высшего руководства до частных рекомендаций, включающих специфические аспекты, для ИТ-руководства.
    - полезность (применимость): информация максимально адаптирована для целей формирования программ совершенствования системы ИТ-управления.

**Основные этапы проведения аудита**

В обобщенном виде ИТ-аудит проводится в два этапа:

* этап "Планирование ИТ-аудита".
* этап "Проведение ИТ-аудита".

На этапе "Планирования ИТ-аудита":

* Анализируются:
  + структура бизнес-процессов;
  + платформы и структура информационных систем, поддерживающих бизнес-процессы;
  + структура ролей и распределения ответственности, включая аутсорсинг;
  + бизнес-риски и бизнес-стратегия.
* Определяются информационные критерии, наиболее значимые для существующих бизнес-процессов.
* Идентифицируются ИТ-риски.
* Оценивается общий уровень контроля рассматриваемых бизнес-процессов.
* На основе полученной информации осуществляется выбор границ и объектов исследования: ИТ-процессов и связанных с ними ИТ-ресурсов.

На этапе "Проведения ИТ-аудита" выполняются следующие виды работ:

* Идентификация существующих механизмов управления и документирование процедур (сбор и первичный анализ информации);
* Оценка эффективности существующих механизмов управления при выполнении задач управления, их целесообразность и пригодность;
* Тест соответствия (получение гарантий пригодности существующих механизмов управления для решения задач управления);
* Детальное тестирование с целью выполнения корректирующих действий для улучшения состояния системы управления ИТ.

**Результаты проведения ИТ-аудита**

Результаты ИТ-аудита компании классифицируются на три группы:

* Организационные – планирование, управление, документооборот функционирования ИС.
* Технические – сбои, неисправности, оптимизация работы элементов ИС, непрерывное обслуживание, создание инфраструктуры и т.д
* Методологические – подходы к решению проблемных ситуаций, управлению и контролю, общая упорядоченность и структуризация.

Проведенный ИТ-аудит позволит обоснованно создать следующие документы:

* **Основные документы:**
* Отчет о результатах ИТ-аудита компании.
* Отчет о результатах аудита информационной безопасности компании.
* **Дополнительные документы** (документы, которые могут быть разработаны по согласованию сторон в дополнение к основным):
* Долгосрочный план развития ИТ/ИС;
* Краткосрочный план развития ИТ/ИС;
* Отчет о текущем состоянии ИТ/ИС.
* Техническое задание на изменение ИТ/ИС
* Методология работы и настройки (доводки) ИТ/ИС компании.
* Концепция построения политики безопасности ИТ/ИС компании.
* Политика безопасности ИТ/ИС компании.
* План восстановления ИТ/ИС в чрезвычайной ситуации.
* Порядок действий в случае нарушения защиты информации.
* План-график проведения последующих ИТ-аудитов.

Результатные документы могут иметь сокращенную и полную редакции. Документ в сокращенной редакции – это документ, содержащий основные итоги и рекомедации по тематике ИТ-аудита и предназначенный для топ-менеджеров компании. Документ в полной редакции – это документ с подробным изложением материала, предназначенный для менеджеров среднего звена и ИТ-спецалистов.