PEMPAL

Аудит в сфере информационных технологий: подготовка, инструменты и практические примеры

Комитас Степанян, PhD, CRISC, CRMA, CobitF
Заместитель директора,
Департамент корпоративных услуг и развития,
Центральный банк Армении

23 ноября 2020

Содержание

- Наиболее важные задания для аудиторов в сфере ИТ
  - Сеть
  - Системы применения
  - Базы данных
  - Информационная безопасность/безопасность в киберпространстве
- Инструменты для выполнения аудиторского задания в сфере ИТ при отсутствии глубоких знаний в области информационных технологий
- Практические примеры

Наиболее важные задания для аудиторов в сфере ИТ: 1 – Сеть

1. Убедиться в документальном отражение процедур
2. Проанализировать порядок исправления уязвимостей в сетевом ПО
3. Проанализировать уязвимости сети с точки зрения безопасности в киберпространстве
4. Выявить процедуры и изменения, связанные с политикой управления сетевыми устройствами защиты
5. Подтвердить защищённость беспроводных сетей
6. Проверить сеть на наличие точек несанкционированного доступа
7. Проанализировать порядок контроля журнала системных событий

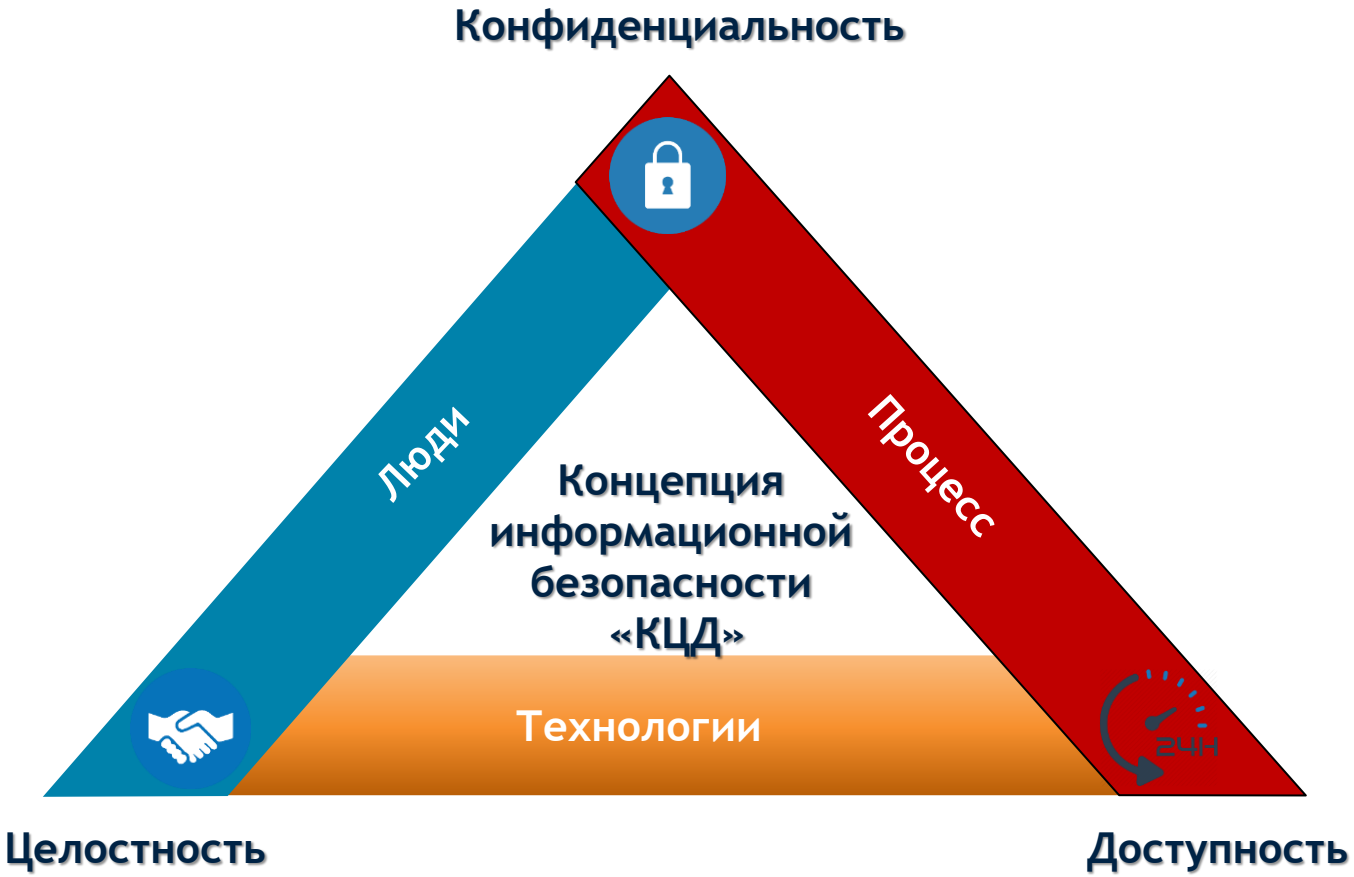
Наиболее важные задания для аудиторов в сфере ИТ : 2 – системы применения

1. Пользователи, группы и права
2. Политика и процедуры обновлений/модернизации, порядок действий после окончания периода получения бесплатных обновлений и бесплатной технической поддержки
3. Управление обновлениями для системы безопасности
4. Управление изменениями
5. Процедуры резервирования и восстановления
6. План преодоления последствий аварийной ситуации

Наиболее важные задания для аудиторов в сфере ИТ : 3 – базы данных

1. Пользователи, группы и права
    1. Учётные записи «по умолчанию» и неудовлетворительные пароли с точки зрения из надёжности
2. Мониторинг активности в учётных записях администраторов базы данных и привилегированных пользователей
3. Политика и процедуры обновлений/модернизации, порядок действий после окончания периода получения бесплатных обновлений и бесплатной технической поддержки
4. Управление изменениями
5. Процедуры резервирования и восстановления

Наиболее важные задания для аудиторов в сфере ИТ: 4 – безопасность в киберпространстве

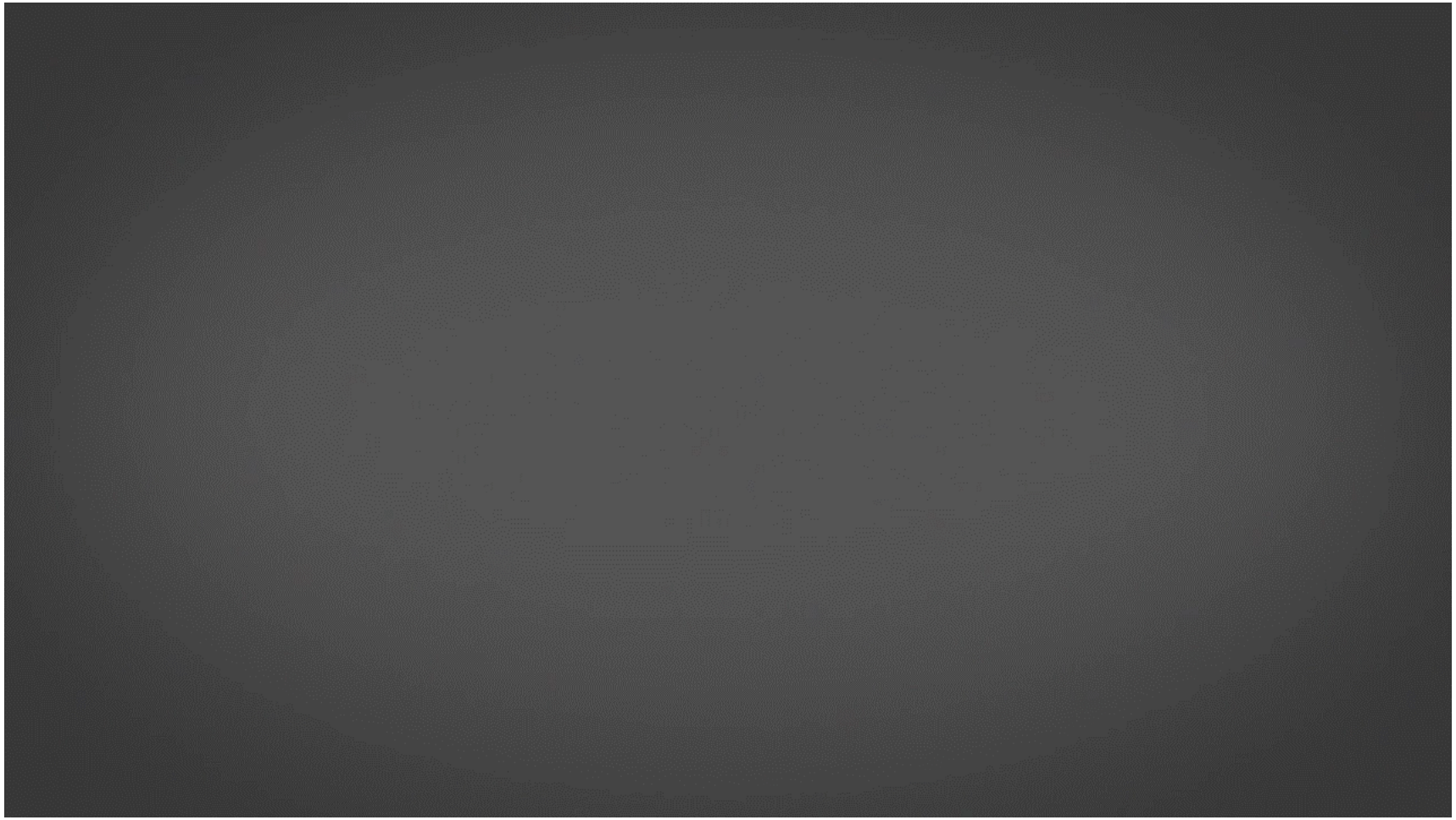


Инструментарий для использования

- **IT Network Inventory -** инструмент инвентаризации сети, обеспечивающий глубокое сканирование
- **Spiceworks Inventory** - инструмент инвентаризации сети, который в автоматическом режиме обнаруживает сетевые устройства
- **Network Inventory Advisor -** инструмент инвентаризации сети
- **Netwrix Auditor -** ПО для проверки безопасности сети с мониторингом конфигурации
- **Nessus -** бесплатный инструмент для анализа уязвимостей, имеющий более 450 шаблонов конфигураций
- **Nmap** - сканер портов и инструмент составления топологии сети с открытым исходным кодом, доступный как командный интерфейс или как графический интерфейс пользователя (Zenmap)
- **OpenVAS** - инструмент оценки уязвимости для пользователей Linux с регулярными обновлениями
- **Acunetix –** инструмент для сетевой проверки безопасности, способный выявить более

  50 000 сетевых уязвимостей; интегрирован с OpenVAS
- **ManageEngine ADAudit Plus -** инструмент аудита для Active Directory, где «зашиты» более 200 стандартных отчётов

Пример – Обнаружение сети



СПАСИБО ЗА ВНИМАНИЕ!