КиберОснова · SGRC-платформа для автоматизации ИБ · sgrc.cyberosnova.ru

Чек-лист инвентаризации ИТ-активов

30 пунктов проверки · Оборудование, ПО, СЗИ, СКЗИ, лицензии

Организация: _____ Дата проверки: ___.___.____ Ответственный: _____

Нормативная база: ISO/IEC 27001:2022 (A.8), Приказы ФСТЭК №17/21/239, 187-ФЗ о КИИ, Приказ ФАПСИ №152 (учёт СКЗИ). Рекомендуемая периодичность: **ежеквартально**.

1. Подготовка к инвентаризации

- ☐ Назначен ответственный за инвентаризацию (приказ руководителя)
  ФИО, должность, номер приказа
- ☐ Определён периметр инвентаризации (филиалы, подразделения, типы активов)
  Весь парк или отдельные площадки?
- ☐ Подготовлен шаблон реестра ИТ-активов (Excel / CMDB)
  Скачать шаблон: sgrc.cyberosnova.ru → Инвентаризация
- ☐ Собрана предыдущая версия реестра (если есть) для сверки
  Сравнить факт vs реестр — выявить расхождения
- ☐ Определён метод сбора данных: ручной / агент / Active Directory / KSC
  Агентный метод — точнее и быстрее

2. Оборудование (Hardware)

- ☐ Серверы: наименование, модель, серийный номер, расположение, ответственный
  Включая виртуальные хосты (ESXi, Proxmox)
- ☐ Рабочие станции (АРМ): модель, инвентарный номер, пользователь, кабинет
  Сверить с бухгалтерским учётом ОС
- ☐ Ноутбуки: наименование, серийный номер, за кем закреплён
  Выносные устройства — повышенный риск утраты
- ☐ Сетевое оборудование: коммутаторы, маршрутизаторы, точки доступа Wi-Fi
  Hostname, IP, модель, расположение, версия прошивки
- ☐ Периферия: принтеры, сканеры, МФУ — особенно с жёсткими дисками
  МФУ могут хранить копии документов на диске!
- ☐ Съёмные носители: USB-диски, флешки, внешние HDD — ведётся ли журнал?
  Обязательно для ИСПДн и КИИ

3. Программное обеспечение

- ☐ Операционные системы: версия, редакция, дата установки, способ лицензирования
  Windows / Linux / Astra Linux / ALT Linux / macOS
- ☐ Офисное ПО: MS Office / LibreOffice — версия, тип лицензии
  Проверить наличие нелицензионного ПО!
- ☐ Прикладное ПО: 1С, CRM, ERP, СУБД, веб-приложения
  Учитывать серверные и клиентские лицензии
- ☐ Лицензии: тип (OEM/подписка/бессрочная), срок действия, количество
  Выделить лицензии с истекающим сроком (менее 3 мес.)
- ☐ Нелицензионное / теневое ПО: проверить наличие неучтённых установок
  Штраф по ст. 7.12 КоАП — до 40 000 ₽ за каждый случай

4. Средства защиты информации (СЗИ)

- ☐ Антивирус: продукт, версия, актуальность баз, количество лицензий
  KES, Dr.Web, ClamAV — проверить покрытие всех АРМ
- ☐ Средства от НСД: Secret Net, Dallas Lock — номер сертификата ФСТЭК, срок
  Сертификат истёк = СЗИ не легитимно для аттестации!
- ☐ Межсетевые экраны: Check Point, UserGate, Континент — версия, лицензия
  Проверить актуальность подписки на обновления IPS/IDS
- ☐ SIEM / SOAR / сканеры уязвимостей: наличие, покрытие
  MaxPatrol, RedCheck, KUMA — для КИИ критично

5. СКЗИ (средства криптозащиты)

По Приказу ФАПСИ №152 — отдельный учёт с журналами

- ☐ Журнал поэкземплярного учёта СКЗИ — актуален, все записи на месте?
  Проверить соответствие факта и записей в журнале
- ☐ Технический (аппаратный) журнал СКЗИ — ведётся для аппаратных СКЗИ?
  Обязателен для криптошлюзов, токенов, HSM
- ☐ Ключевые документы — учтены? Не просрочены ли сертификаты КЭП?
  Проверить сроки ключей во всех подразделениях
- ☐ Сертификаты ФСБ/ФСТЭК на СКЗИ — действительны? Не отозваны?
  Проверить на сайте ФСБ / реестр ФСТЭК

6. Финализация и отчёт

- [ ] Реестр ИТ-активов заполнен и актуализирован
  Все поля заполнены, нет пустых строк
- [ ] Выявлены расхождения с предыдущей версией реестра
  Новые активы, списанные, перемещённые
- [ ] Составлен список активов с истекающими лицензиями / сертификатами
  Передать в закупки для продления
- [ ] Проверена принадлежность активов к ИСПДн / ГИС / КИИ
  Для КИИ — обязательно отметить в реестре
- [ ] Акт инвентаризации подписан ответственным и руководителем
  Хранить не менее 5 лет