Чек-листы для аудита помогают систематизировать процесс проверки и убедиться, что все необходимые аспекты были учтены. Для удобства разделим на два типа: для внутреннего аудита (проводимого специалистом внутри организации) и для внешнего аудита (проводимого внешней организацией).

**1. Чек-лист для специалиста внутри организации**

Этот чек-лист направлен на предварительную оценку текущего состояния информационной безопасности (ИБ) внутри компании и служит для подготовки к внешнему аудиту или сертификации.

**1.1 Политики и процедуры**

* Есть ли утвержденная политика информационной безопасности (ИБ)?
* Проводится ли регулярное обновление и актуализация политики ИБ?
* Есть ли документированные инструкции по управлению инцидентами?
* Назначены ли ответственные лица за реализацию и контроль выполнения политики ИБ?

**1.2 Управление доступом**

* Применяются ли средства двухфакторной аутентификации (2FA)?
* Ограничены ли привилегированные доступы только для необходимых пользователей?
* Проводится ли регулярная проверка актуальности прав доступа пользователей?
* Зафиксированы ли политики использования паролей (например, длина, регулярность смены)?

**1.3 Инфраструктура и сетевые устройства**

* Ведется ли инвентаризация оборудования (серверов, ПК, сетевых устройств)?
* Обеспечена ли сегментация сети?
* Обновляется ли программное обеспечение и прошивки на всех устройствах?
* Используются ли межсетевые экраны и системы обнаружения вторжений (IDS/IPS)?

**1.4 Физическая безопасность**

* Установлены ли системы контроля физического доступа (СКУД)?
* Обеспечена ли охрана серверных помещений (видеонаблюдение, сигнализация)?
* Хранится ли оборудование в защищенных местах?

**1.5 Реагирование на инциденты**

* Есть ли команда, отвечающая за реагирование на инциденты?
* Проводятся ли тренировки реагирования на кибератаки или утечки данных?
* Ведется ли журнал инцидентов ИБ и их последствий?

**1.6 Управление уязвимостями**

* Проводится ли регулярное сканирование на уязвимости?
* Выполняется ли оперативная установка патчей безопасности?
* Проводится ли анализ новых уязвимостей и контроль за их устранением?

**2. Чек-лист для внешней организации**

Этот чек-лист помогает внешней аудиторской компании оценить соответствие организации нормативным требованиям и стандартам в области информационной безопасности.

**2.1 Политики и процедуры**

* Соответствует ли политика информационной безопасности требованиям законодательства и стандартов (например, ФЗ-152, ISO/IEC 27001)?
* Установлены ли процедуры управления рисками и уязвимостями?
* Прописаны ли роли и обязанности по защите данных и управлению инцидентами?

**2.2 Комплаенс и нормативные требования**

* Соответствует ли организация требованиям ФСТЭК, ФСБ и других регулирующих органов?
* Есть ли документальные доказательства соответствия стандартам (например, сертификаты)?
* Проводятся ли регулярные проверки и тестирования на соответствие требованиям законодательства?

**2.3 Управление инцидентами**

* Установлены ли и документированы ли процедуры реагирования на инциденты (инструкции, план действий)?
* Есть ли политика уведомления регулирующих органов в случае утечки персональных данных?
* Проводился ли аудит инцидентов за последние 12 месяцев?

**2.4 Защита данных**

* Используются ли криптографические методы защиты данных при передаче и хранении?
* Применяются ли меры защиты персональных данных в соответствии с требованиями ФЗ-152?
* Есть ли меры по защите данных в облачных системах, если они используются?

**2.5 Управление доступом и аутентификация**

* Проверяются ли логины пользователей для предотвращения несанкционированного доступа?
* Используются ли процедуры блокировки учетных записей после нескольких неудачных попыток входа?
* Настроены ли политики минимальных прав (пользователи получают только те права, которые необходимы)?

**2.6 Инвентаризация и управление активами**

* Ведется ли журнал всех ИТ-активов, включая оборудование, программное обеспечение и сетевые устройства?
* Проводятся ли регулярные аудиты активов (проверка актуальности данных, наличия оборудования)?
* Обеспечен ли контроль доступа к критическим ИТ-активам?

**2.7 Управление сетевой безопасностью**

* Осуществляется ли фильтрация трафика с использованием межсетевых экранов?
* Есть ли системы обнаружения вторжений (IDS/IPS) и настроены ли они корректно?
* Защищены ли сети от атак DDoS и других типов сетевых угроз?

**2.8 Физическая безопасность**

* Существует ли политика доступа к серверным помещениям и другим критическим объектам?
* Есть ли меры по защите от краж оборудования (замки, сейфы, контроль доступа)?
* Ведется ли мониторинг физических помещений с использованием камер видеонаблюдения?

**2.9 Обучение и повышение осведомленности персонала**

* Проводятся ли регулярные тренинги и обучение по информационной безопасности для сотрудников?
* Есть ли программы по повышению осведомленности сотрудников о киберугрозах и безопасной работе с данными?
* Участвуют ли сотрудники в учениях по реагированию на инциденты?

**Заключение**

Чек-листы помогают систематизировать процесс аудита как внутри организации, так и внешними аудиторами. Внутренний чек-лист помогает готовить компанию к внешнему аудиту, а внешний — проверять соответствие нормативным требованиям и лучшим практикам в области ИБ.