Опросные листы для организации используются для сбора информации, необходимой для проведения аудита информационной безопасности. Они помогают систематизировать информацию и обеспечить полноту данных для анализа. Вот примеры опросных листов для различных аспектов информационной безопасности:

**1. Опросный лист для оценки политики и процедур**

**1.1 Политики безопасности**

* Существуют ли в организации документированные политики информационной безопасности?
* Как часто обновляются политики?
* Кто отвечает за разработку и утверждение политик?

**1.2 Процедуры и стандарты**

* Какие процедуры безопасности внедрены (например, управление доступом, реагирование на инциденты)?
* Как часто проводятся тренинги и обучения по этим процедурам?

**1.3 Организация и управление**

* Назначены ли ответственные лица за соблюдение политик безопасности?
* Как осуществляется контроль за соблюдением политик?

**2. Опросный лист для оценки инфраструктуры и архитектуры**

**2.1 Инвентаризация оборудования**

* Какие серверы, рабочие станции и сетевые устройства используются в организации?
* Как ведется учет и управление оборудованием?

**2.2 Программное обеспечение**

* Какое программное обеспечение установлено на системах?
* Используются ли лицензированные версии программного обеспечения?

**2.3 Архитектура сети**

* Какова топология сети и какие основные компоненты в нее входят?
* Как обеспечивается сегментация сети?

**3. Опросный лист для оценки управления доступом**

**3.1 Управление пользователями**

* Как осуществляется создание и удаление учетных записей пользователей?
* Как управляются права доступа пользователей?

**3.2 Аутентификация и авторизация**

* Какие методы аутентификации используются (пароли, двухфакторная аутентификация и т.д.)?
* Как проверяется соответствие прав доступа требованиям безопасности?

**3.3 Мониторинг и аудит**

* Как проводится мониторинг доступа к системам и данным?
* Какие отчеты генерируются и как они анализируются?

**4. Опросный лист для оценки физической и логической безопасности**

**4.1 Физическая безопасность**

* Какие меры физической безопасности приняты (контроль доступа, видеонаблюдение)?
* Как обеспечивается защита оборудования от несанкционированного доступа?

**4.2 Логическая безопасность**

* Какие системы защиты от внешних и внутренних угроз используются (межсетевые экраны, системы обнаружения вторжений)?
* Как обеспечивается безопасность данных при передаче и хранении?

**5. Опросный лист для оценки управления инцидентами**

**5.1 Процедуры реагирования на инциденты**

* Существуют ли документированные процедуры для реагирования на инциденты безопасности?
* Как осуществляется уведомление и отчетность о происшествиях?

**5.2 История инцидентов**

* Какие инциденты безопасности произошли за последний год?
* Какие меры были предприняты для их устранения и предотвращения повторения?

**6. Опросный лист для оценки управления уязвимостями**

**6.1 Анализ уязвимостей**

* Как проводится регулярный анализ уязвимостей системы?
* Какие инструменты и методики используются для выявления уязвимостей?

**6.2 Обновления и патчи**

* Как осуществляется управление обновлениями и патчами программного обеспечения?
* Как проверяется эффективность установленных обновлений?

**Примеры вопросов для опросных листов:**

**1. Политики и процедуры:**

* Есть ли у вас документированная политика безопасности? Да/Нет
* Когда последний раз пересматривалась политика безопасности? [Дата]

**2. Инфраструктура:**

* Перечислите основные серверы и их роли в сети.
* Какой тип брандмауэра используется для защиты сети?

**3. Управление доступом:**

* Какие методы аутентификации используются для доступа к критическим системам?
* Как осуществляется проверка и изменение прав доступа?

**4. Физическая безопасность:**

* Как осуществляется контроль доступа в серверные комнаты?
* Какие меры приняты для защиты от физического вмешательства?

**5. Управление инцидентами:**

* Какой процесс реагирования на инциденты безопасности используется в вашей организации?
* Как часто проводятся тренинги по реагированию на инциденты?

Эти опросные листы можно адаптировать под конкретные потребности вашей организации и аудитора.