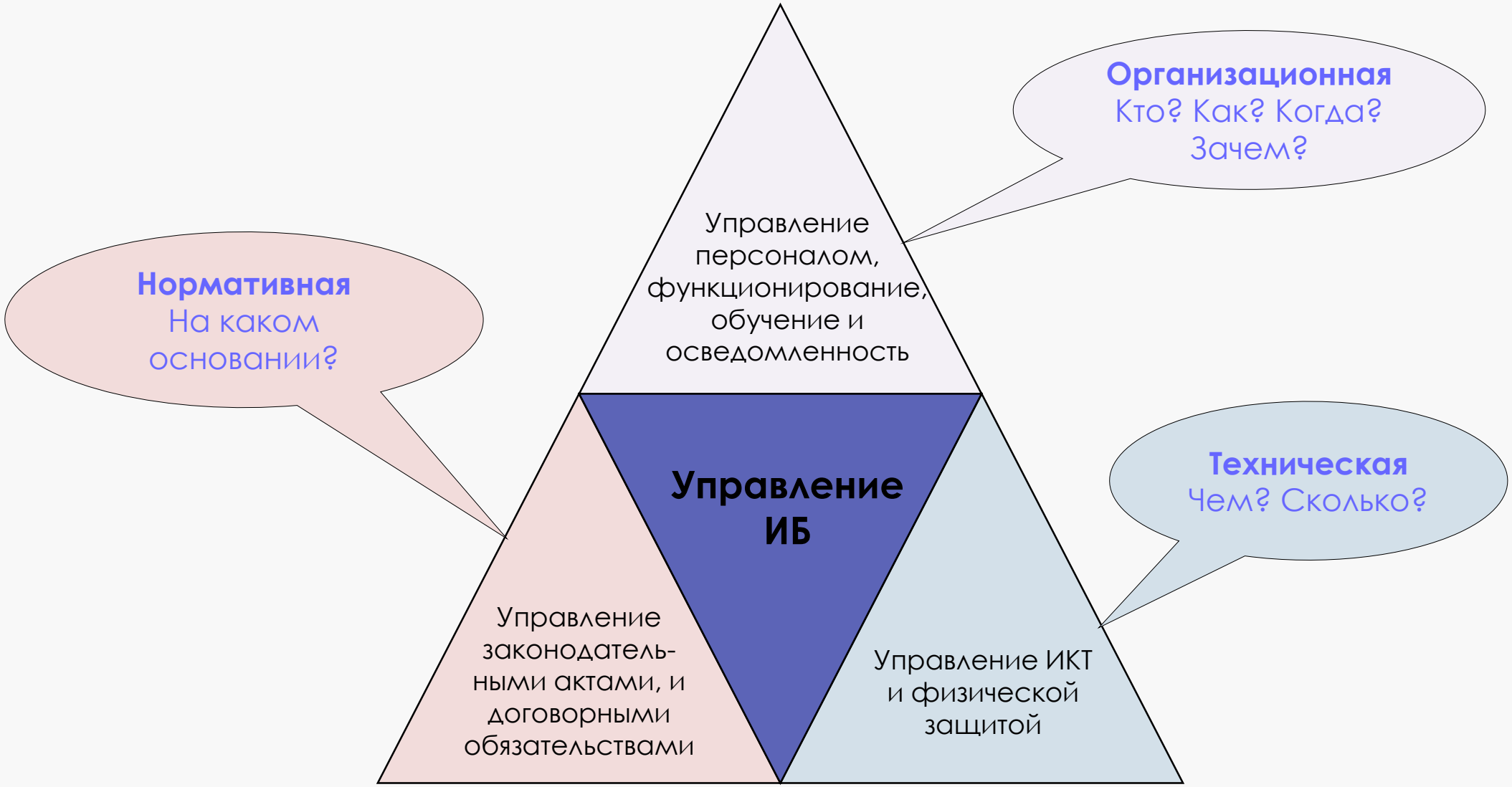
ICORE

Обследование ИТ-инфраструктуры(ИТ)

Система Управления Информационной Безопасностью охватывает 3 области:

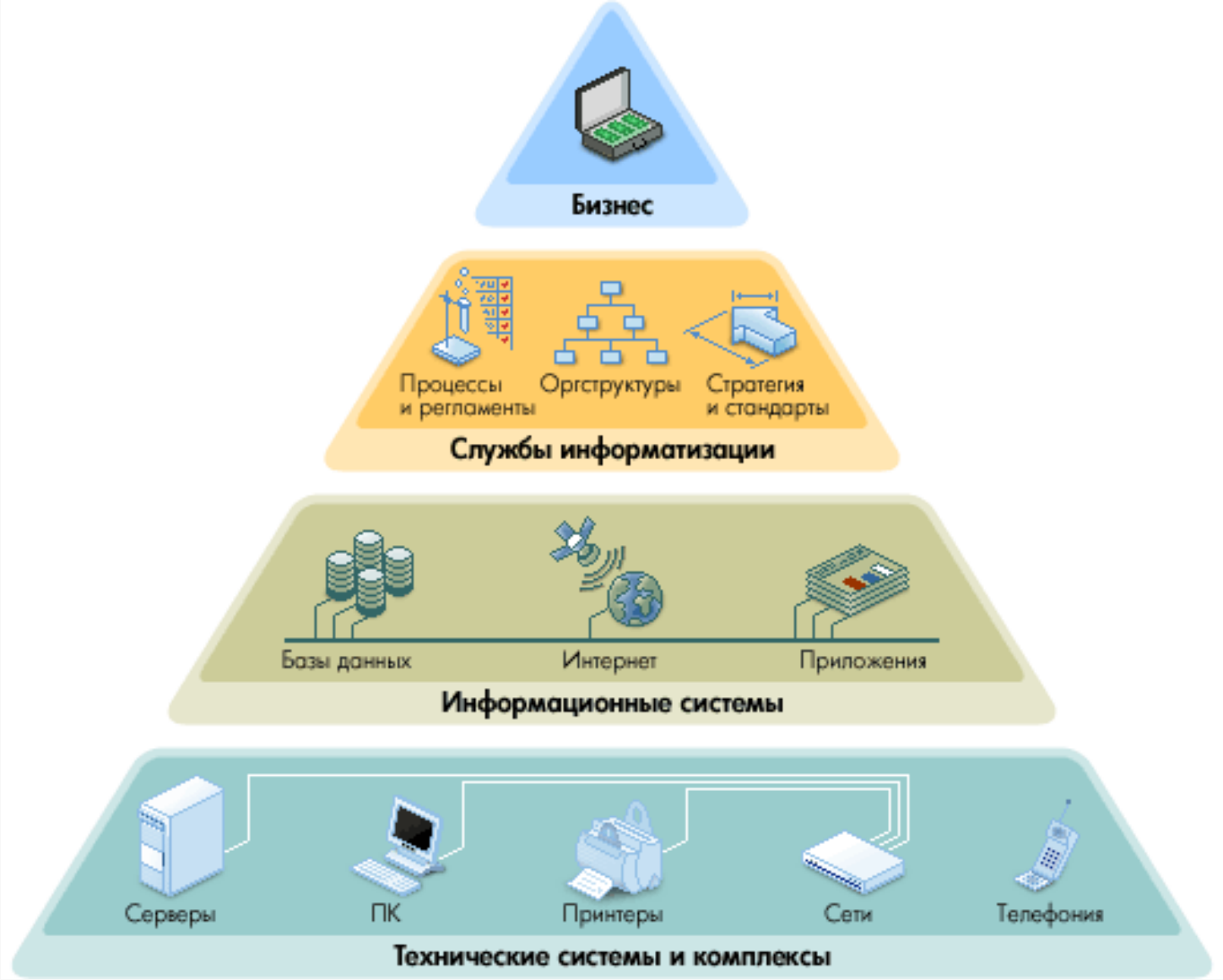


Обследование или аудит?

Аудит - систематический, независимый и документированный процесс получения свидетельства аудита и объективной его оценки с целью определения степени, с которой выполняются критерии аудита (ISO 27000).

Обследование - оценка текущего уровня ИТ инфраструктуры организации с разработкой рекомендаций по реализации комплекса организационных и технических мер, повышающих существующий уровень ИТ инфраструктуры.

Модель архитектуры информационных технологий



Цели услуги Обследование ИТ и ее ценность для Заказчика

Цели ИТ обследования формируются в зависимости от обьекта контроля (ИТ-инфраструктура, ИТ менеджмент, ИТ услуги, ИС) с учетом взаимосвязи с циклом Деминга. Основными целями проведения ИТ обследования является:

1. Оценка эффективности расходуемого на ИТ инфраструктуру бюджета
2. Оценка эффективности работы ИТ-отдела, а также общий уровень подготовки кадров.
3. Определить места в инфраструктуре и бизнес-процессах, где ИТ-системы используются недостаточно эффективно, выработать рекомендации по повышению эффективности, перераспределению нагрузки

Кроме того, в ходе Обследования выявляются возможные риски для предприятия и способы их минимизации. Например, текущее серверное оборудование уже неактуально (последние версии операционной системы его не поддерживает) и рекомендуется заменить.

Задачи услуги Обследование ИТ и ее ценность для Заказчика

1. Получение объективной независимой экспертной оценки текущего состояния ИТ-инфраструктуры и технических средств обеспечения ИБ
2. Анализ топологии телекоммуникационных сетей состава и характеристик аппаратных программных технических средств
3. Анализ существующей ситуации компонентов ИТ-инфраструктуры, включая технические средства обеспечения ИБ
4. Оценка эффективности сопровождения и технической поддержки информационных систем
5. Инструментальное сканирование компонентов ИТ-инфраструктуры на наличие уязвимостей, их ручной анализ
6. Выработка рекомендаций по совершенствованию и автоматизации технических средств обеспечения ИБ и по устранению выявленных критичных уязвимостей

Процесс оказания услуги по Обследованию ИТ

1. Интервьюирование ключевых лиц, ответственных за ИТ, за управление и обеспечение ИБ, а также работников, отобранных для участия в опросах;

2. Анализ топологии телекоммуникационных сетей, состава и характеристик аппаратных и программных технических средств;

3. Анализ существующей конфигурации компонентов ИТ-инфраструктуры, включая технические средства обеспечения ИБ;

4. Инструментальное сканирование компонентов ИТ-инфраструктуры на наличие уязвимостей, их ручной анализ;

5. Выработка рекомендаций по развитию и техническому дооснащению ИТ/ИБ инфраструктуры;

6. Выработка рекомендаций по совершенствованию и автоматизации технических средств обеспечения ИБ;

7. Создание актуальной на момент проведения обследования схемы сети и рекомендуемой схемы сети;

8. Формирование рекомендаций по устранению выявленных критичных уязвимостей;
расчёт затрат на модернизацию ИТ/ИБ инфраструктуры.

Границы услуги Обследование ИТ

Формируются на основании:

- информации из Опросника
- результатов аудитов, ИТ обследования (при наличии)

Границами услуги являются:

- Беспроводная сеть,
- внутренние коммуникации,
- внешние коммуникации,
- центр обработки данных,
- конечные устройства,
- приложения (инфраструктурные и корпоративные),
- управление ИТ-инфраструктурой,
- технические меры по обеспечению ИБ,
- работники, отобранные для участия в опросах.

Результаты услуги Обследование ИТ :

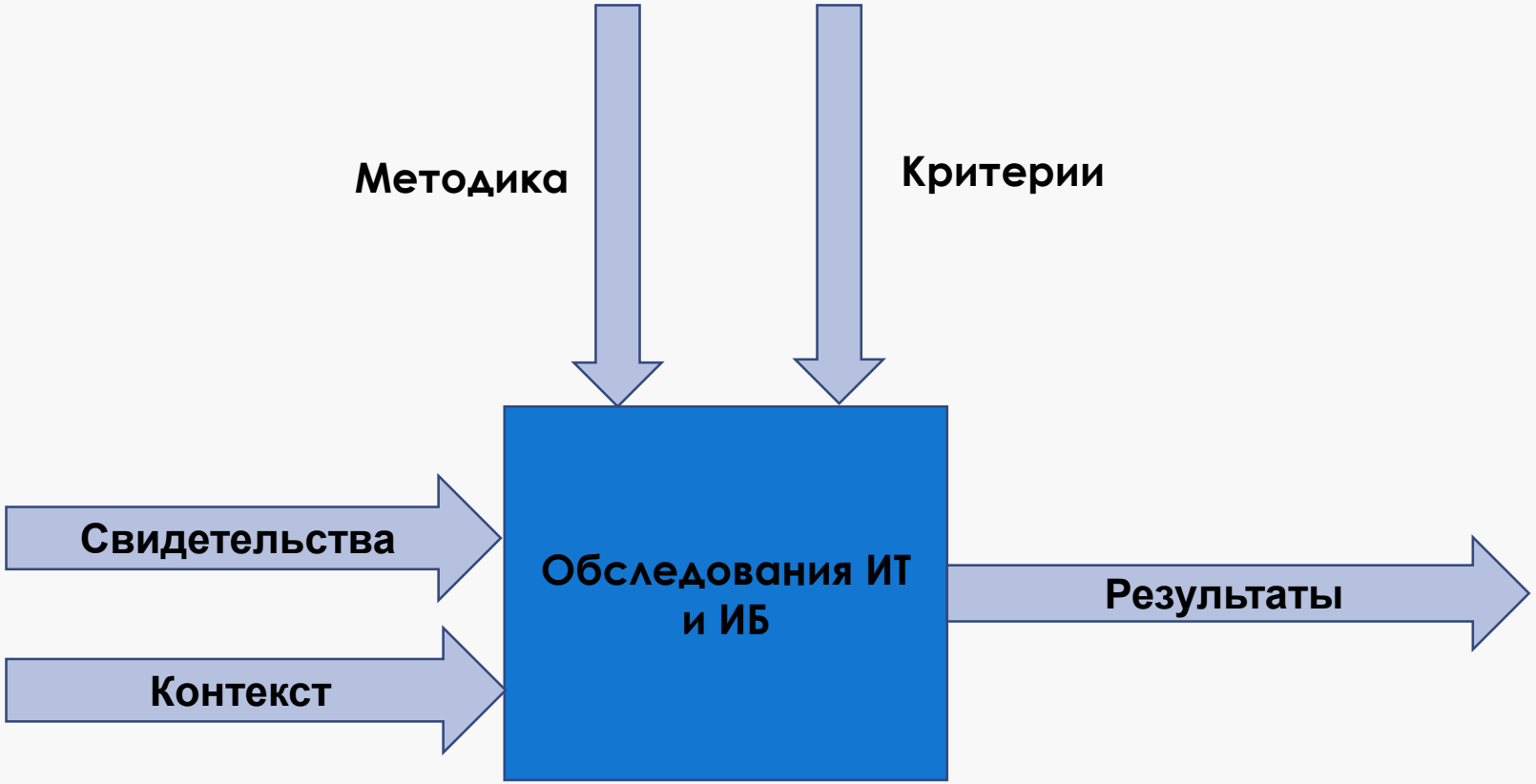
- Технический отчет на русском языке с оценкой текущего состояния ИТ-инфраструктуры, с учетом требований ИБ, включающий в себя:
  1)описание каждого элемента ИТ-инфраструктуры,
  2)технологическую модель ИТ-инфраструктуры (существующей и рекомендуемую),
  3)бюджетную оценку по оптимизации и развитию ИТ-инфраструктуры.

- Отчеты о выявленных уязвимостях (отчет, сформированный из автоматизированной системы оценки уязвимости включающий ручной анализ и рекомендации по устранения уязвимостей);

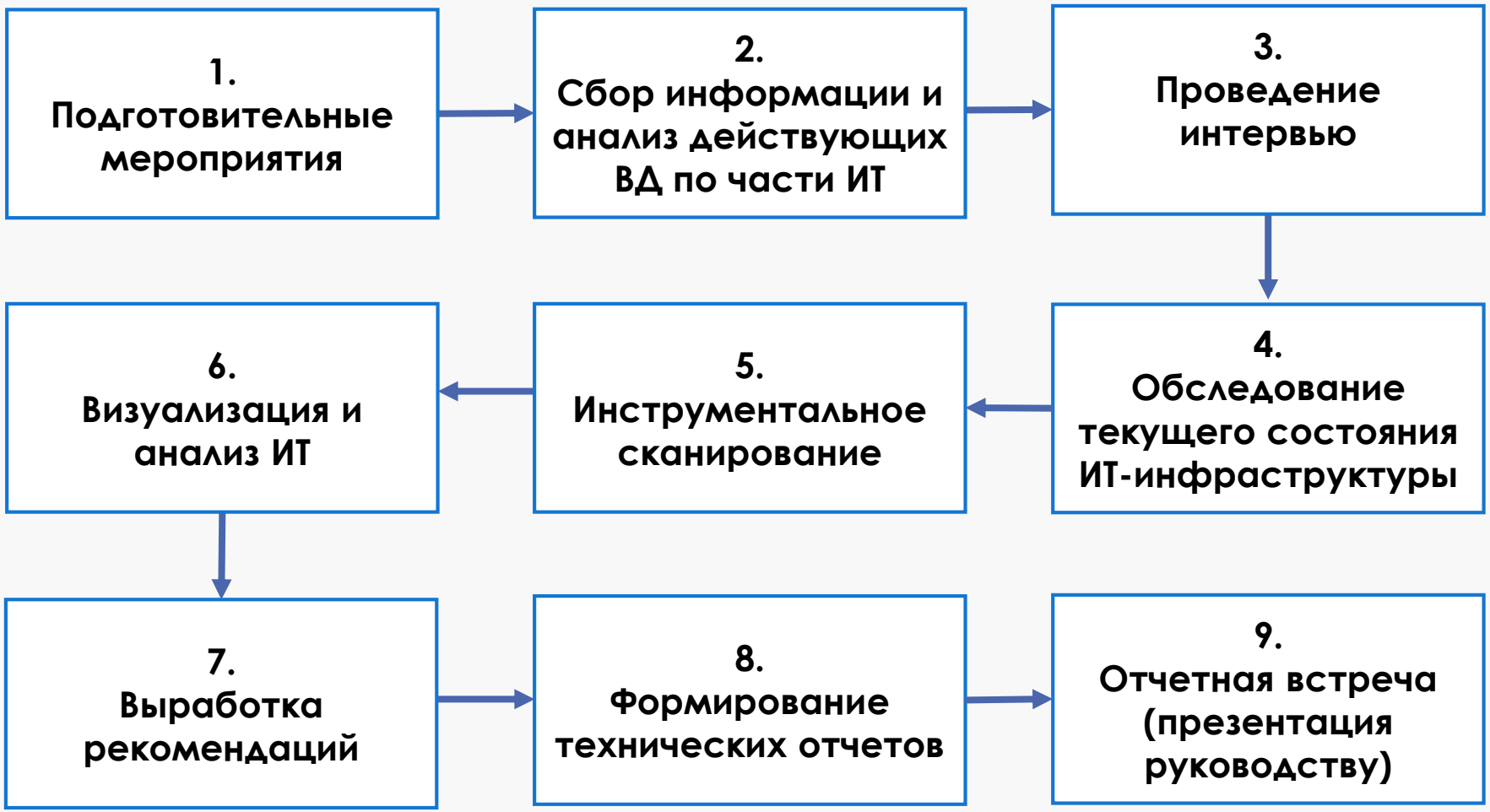
- Диск с электронными копиями отчетов, включая схемы и иные документы (дизайн схемы действующей и рекомендуемой сети, таблицы, графики, презентации, отчеты о выявленных уязвимостях);

- Резюме для высшего руководства в виде слайдов презентации, содержащее краткие итоги работ;

Общая модель Услуг

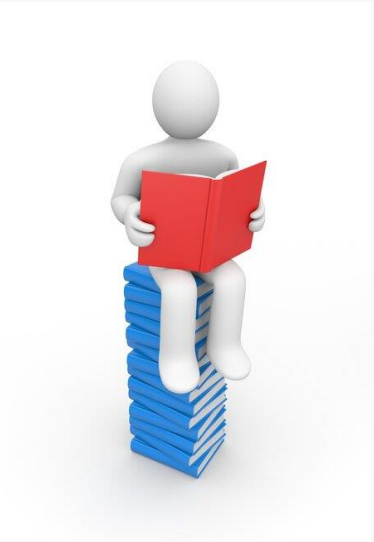


Этапы работ по Обследованию ИТ



1. Подготовительные мероприятия

1. Получение поддержки от руководства Заказчика путем формирования организационно-распорядительного документа (Приказа/Распоряжения) о начале проекта на основании предоставленного Исполнителем шаблона (сроки, ответственный за проект со стороны Заказчика, рабочая группа, их роли);
2. Получение и изучение функционально-организационной схемы Заказчика (оргструктура, штатное расписание, корпоративный телефонный справочник);
3. Составление и согласование формы Протокола разногласий;
4. Получение списка действующих ВД, определение и запрос необходимых для анализа ВД;
5. Формирование и согласование Плана проекта, сроков проведения работ;
6. Определение лиц, ответственных за управление процессами ИБ.



2. Сбор информации и анализ действующих ВД по части ИТ

1. Получение необходимых действующих ТД, включая свидетельства (записи) применения механизмов контроля в IT-инфраструктуре (схемы и конфигурации сетей, оборудования, виртуализации, операционных систем, бизнес систем, ИБ системы);

2. Определение лиц, ответственных за сопровождение ИТ-инфраструктуры и технических средств обеспечения ИБ

3. Интервью

1. Формирование и согласование с ответственны за проект со стороны Заказчика Методики и Плана-графика проведения интервьюирований с работниками ответственными за ИТ-инфраструктуру Заказчика, которые будут участвовать в опросах;
2. Проведение интервью с ответственными работниками за ИТ-инфраструктуру согласно План-графику для заполнения соответствующих разделов опросника;
3. Ознакомление и подписание заполненных анкет интервьюированными лицами;
4. Наблюдения и опрос работников Заказчика для подтверждения объективных свидетельств выполнения применимых требований и положений междударных стандартов в ИТ-сфере и «лучших практик».

4. Обследование ИТ-инфраструктуры

Проведение обследования сетевой инфраструктуры включает:

1) сетевой инфраструктуры
2) сети беспроводной передачи данных
3) систем телефонии и конференций
4) внешнего сетевого периметра
5) ЦОД
6) конечных устройств
7) платформы серверной виртуализации, критичных бизнес-приложений и информационных систем
8) технических средств обеспечения ИБ

Разработка рекомендации по устранению/минимизации выявленных несоответствий, включая рекомендации по совершенствованию и автоматизации технических средств обеспечения ИБ.

4.1. Обследование сетевой инфраструктуры

- обследование архитектуры построения сети передачи данных,
- анализ конфигурационных файлов сетевых устройств,
- анализ топологии сети, состава и характеристик программных и аппаратных средств,
- инвентаризация активного и пассивного оборудования,
- разработка рекомендуемого дизайна сети с учетом “лучших практик”

4.2. Обследование сети беспроводной передачи данных

- описание текущих характеристик беспроводной сети,
- проверка беспроводной сети на безопасность,
- выработка рекомендации по устранению недостатков.

4.3. Обследование систем телефонии и конференции

- обследование систем телефонии с точки зрения безопасности,
- описание сетевых настроек системы телефонии,
- описание настроек систем конференцсвязи,
- разработка рекомендаций по устранению недостатков.

4.4. Обследование внешнего сетевого периметра

- обследование оборудования внешнего сетевого периметра,
- описание организации удаленного доступа,
- анализ конфигурационных файлов оборудования,
- описание текущего состояния,
- выработка рекомендаций по устранению недостатков.

4.5. Обследование ЦОДа

- описание текущего состояния инженерных систем Центра обработки данных,
- описание серверной и сетевой инфраструктуры,
- анализ конфигурационных файлов оборудования,
- описание текущего состояния,
- разработка рекомендаций по устранению замечаний.

4.6. Обследование конечных устройств

- проверка с точки зрения безопасности и отказоустойчивости,

- инвентаризация установленных ПО и ОС,

- выработка рекомендации по устранению недостатков.

Обследование конечных устройств, должно быть сформировано согласно минимально-достаточному количеству в размере не более 20% от общего количества.

4.7. Обследование платформы серверной виртуализации, критичных бизнес-приложений и ИС

- обследование гипервизоров платформы серверной виртуализации и системы управления гипервизорами(например: VMware, Hyper-V и т.д.);
- обследование службы каталогов Microsoft Active Directory;
- обследование службы доставки электронной почты;
- выработка рекомендации по устранению недостатков.

4.8. Обследование технических средств обеспечения ИБ

- обследование программно-технических средств обеспечения ИБ: базовые (встроенные механизмы ИБ в сетевую и беспроводную инфраструктуру, телефонию, конечные устройства и приложения) и специализированные (антивирусные средства, DLP, SIEM, NGFW, IDM, PAM, SOAR, WAF),

- анализ эффективности внедренных программно-технических средств ИБ.

5. Инструментальное сканирование

- Сканирование минимум 2 (двумя) проприетарными автоматизированными системами оценки уязвимостей различных производителей:
  - сканирование внешних IP-адресов (все бизнес-системы, сервисы и сетевые узлы) на наличие уязвимостей и слабых мест доступных с внешнего периметра,
  - сканирование внутренних IP-адресов на наличие уязвимостей и слабых мест во внутренней сети (все бизнес-системы и сервисы, сетевые узлы, сервера и не менее 10% конечных рабочих станций);
- Ручной анализ выявленных уязвимостей и разработка методических указаний по устранению выявленных критичных уязвимостей в ИТ-инфраструктуре.

Критичность найденных слабых мест оценивается качественно по шкалам согласно стандартам CVSS 3.0/ CVSS 2.0.

6. Визуализация и анализ ИТ

Создание актуальной на момент проведения обследования физико-логической схемы сети.

Анализ топологии телекоммуникационных сетей, состава и характеристик аппаратных и программных технических средств, эффективности внедренных технических средств обеспечения ИБ.

Создание схем согласно рекомендованному дизайну.

Ручная аналитика выявленных уязвимостей и разработка методических указаний по устранению критичных уязвимостей в ИТ-инфраструктуре.

7. Выработка рекомендаций

После проведения анализа ИТ инфраструктуры разрабатываются рекомендаций по:

– оптимизации ИТ-инфраструктуры, физической и кибербезопасности,

– закрытию выявленных уязвимостей,

– устранению слабостей и недочетов в системах защиты с учетом «лучших практик» и международных стандартов.

8. Формирование технических отчетов

На основании выработанных рекомендаций формируется предварительная бюджетная оценка на программные и аппаратные комплексы.

Данная консолидированная информация формируются в технический отчет описывающий элементы ИТ-инфраструктуры и анализ расчета затрат на модернизацию ИТ/ИБ инфраструктуры

Электронная копия отчетов записывается на диск, включая схемы и иные документы (дизайн схемы действующей и рекомендуемой сети, таблицы, графики, презентации, отчеты о выявленных уязвимостях);

9. Отчетная встреча

-Консультирование Ответственных работников Заказчика по вопросам организации и управление процессами ИТ-инфраструктурой в течении 3-х месяцев с момента подписания акта выполненных работ,

- Консультирование бизнес-владельцев разработанных/актуализированных проектов ВД в процессе согласования ВД с заинтересованными структурными подразделениями Заказчика.

Почему стоит работать с ICORE?

1. При оказании услуг, высококвалифицированные специалисты «ICORE-Consulting» придерживаются процессного, риск-ориентированного подходов, стандартов по управлению проектами и качеством (ISO 31000, ISO 21500, ISO 10005, ISO 9001).
2. Безопасный портал для отчетности и отслеживания проекта
3. Собственная команда квалифицированных аудиторов и отраслевых экспертов-консультантов
4. Строгая политика конфиденциальности
5. Независимая от поставщиков компания
6. Политика отсутствия аутсорсинга
7. Строгие сроки с четко определенным планом проекта и SLA
8. Прозрачность в рабочем процессе
9. Так как информационная безопасность является динамично развивающейся областью, наши специалисты постоянно в курсе современных угроз, уязвимостей и ситуации в бизнес-процессах и технологиях
10. Более 10 лет опыта и знаний в отрасли, более 30 успешно реализованных проектов по консалтингу
11. Сочетание отличного качества и приемлемой стоимости

Спасибо!

ТОО «ICORE-Integraion»
Телефон: +7 (727) 338 55 55

Адрес: Казахстан, 050000, г.Алматы,
бульвар Бухар Жырау 27/5Б

email: sdp@icore.kz
web: www.icore.kz