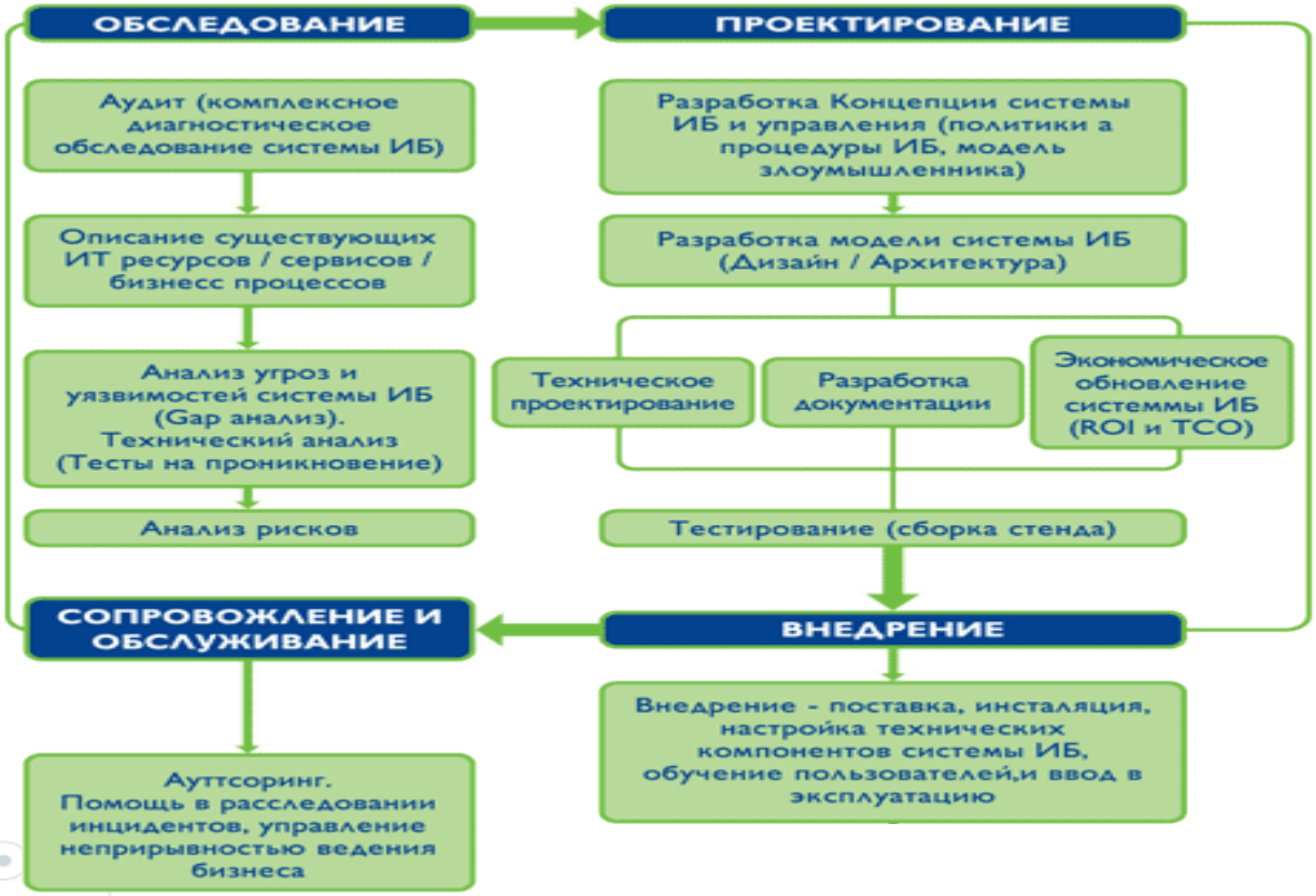
КАК ПОСТРОИТЬ ЭФФЕКТИВНУЮ СИТЕМУ ЗАЩИТЫ ИНФОРМАЦИИ

Грецкий Антон
Ведущий специалист по Информационной безопасности
ActiveCloud
+375336922304
anton.hretski@activecloud.com

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ


PASSWORD

Цикл работ по обеспечению ИБ



Диагностическое обследование/аудит системы ИБ

- **Предпроектное диагностическое обследование** (выполняется при модернизации или построении системы ИБ).

- **Аудит системы ИБ** (или системы управления ИБ) на соответствие требованиям внутрикорпоративным стандартам или международным/национальным стандартам.

- **Специальные виды обследования**, например, при расследовании компьютерных инцидентов.

Интегрированная архитектура системы ИБ

Включает в себя набор следующих подсистем:

- подсистему защиты периметра сети и межсетевых взаимодействий;
- подсистему защиты серверов сети;
- средства защиты рабочих станций;
- подсистему мониторинга и аудита безопасности;
- средства обнаружения атак и автоматического реагирования;
- подсистему комплексной антивирусной защиты;
- средства анализа защищенности и управления политикой безопасности;
- средства контроля целостности данных;
- средства криптографической защиты информации;
- инфраструктуру открытых ключей;
- подсистему резервного копирования и восстановления данных;
- автоматизированную систему установки обновлений ПО;
- средства управления безопасности;
- подсистему аутентификации и идентификации.

Этапы проектирования системы ИБ

1.Разработка Концепции обеспечения информационной безопасности.
2. Создание / развитие политики ИБ.
3. Построение модели системы управления ИБ (на основе процессно-ролевой модели).
4. Подготовка технического задания на создание системы информационной безопасности.
5. Создание модели системы ИБ.
6.Разработка техническо-рабочего проекта (ТРП) создания системы ИБ и архитектуры системы ИБ.

Этапы проектирования системы ИБ

ТРП по созданию системы ИБ включает следующие документы:

- Пояснительную записку
- Обоснование выбранных компонентов системы ИБ и определение мест их размещения.
- Описание разработанных профилей защиты.
- Спецификацию на комплекс технических средств системы ИБ.
- Спецификацию на комплекс программных средств системы ИБ.
- Определение настроек и режима функционирования компонентов системы.

7. Тестирование на стенде спроектированной системы ИБ.
8. Разработка организационно-распорядительных документов системы управления ИБ (политик по обеспечению информационной безопасности, процедур, регламентов и др.).
9. Разработка рабочего проекта (включая документацию на используемые средства защиты и порядок администрирования, план ввода системы ИБ в эксплуатацию и др.), планирование обучения пользователей и обслуживающего персонала информационной системы.

Внедрение системы ИБ

Работы по внедрению системы включают выполнение следующих задач:

- поставку программных и технических средств защиты информации;
- инсталляцию программных компонентов;
- настройку всех компонентов и подсистем;
- проведение приемо-сдаточных испытаний;
- внедрение системы управления ИБ;
- обучение пользователей;
- ввод системы ИБ в промышленную эксплуатацию.

Для эффективной дальнейшей эксплуатации системы необходимы поддержка и сопровождение.

Как выбрать исполнителя?

- компания-консультант должна иметь хорошую репутацию на рынке;
- необходимо убедиться в обширном опыте работы в сфере ИБ как самой компании-консультанта, так и конкретных сотрудников, задействованных в проекте;
- необходимо наличие у исполнителя программно-аппаратных средств для построения тестовых стендов, проведения работ по проектированию и моделированию системы ИБ.

Дополнительные выгоды принесет наличие
у исполнителя высоких партнерских статусов
с поставщиками программно-аппаратных комплексов.

Грецкий Антон

Ведущий специалист по
Информационной безопасности

+375 33 6922304

anton.hretski@activecloud.com