

Основные принципы безопасности (CIA Triad)

Понимание основных принципов безопасности — ключевой элемент для любого архитектора. Одной из наиболее известных моделей в этой области является модель CIA Triad, которая включает в себя три основных компонента: Конфиденциальность, Целостность и Доступность. Эти три принципа помогут вам создать систему, которая не только защищена от внешних и внутренних угроз, но и оптимизирована для выполнения бизнес-задач.

Конфиденциальность

1. **Определение:** Конфиденциальность обеспечивает, что доступ к данным ограничен и возможен только для уполномоченных лиц
2. **Примеры нарушений и угроз:**
 - Фишинговые атаки
 - Утечки данных из-за несоблюдения правил хранения

Целостность

1. **Определение:** Целостность гарантирует, что данные остаются неповрежденными и неизменными во время их обработки и хранения.
2. **Примеры нарушений и угроз:**
 - Атаки с подменой данных (Man-in-the-Middle)
 - SQL Injection

Доступность

1. **Определение:** Доступность обеспечивает непрерывный и стабильный доступ к данным и ресурсам системы.
2. **Примеры нарушений и угроз:**

- DDoS-атаки
- Ошибки в коде, приводящие к сбоям системы

Обеспечение конфиденциальности, целостности и доступности — это не просто технические задачи. Это вопросы, которые требуют комплексного подхода, включая организационные меры, процессы и культуру компании. В роли архитектора вы играете ключевую роль в реализации этих принципов на всех этапах жизненного цикла проекта.

Возможно, если вы в крупной корпорации и работаете с существующей системой - все стандарты безопасности уже придуманы до вас, но вы также можете посмотреть на них свежим взглядом и предложить изменения.