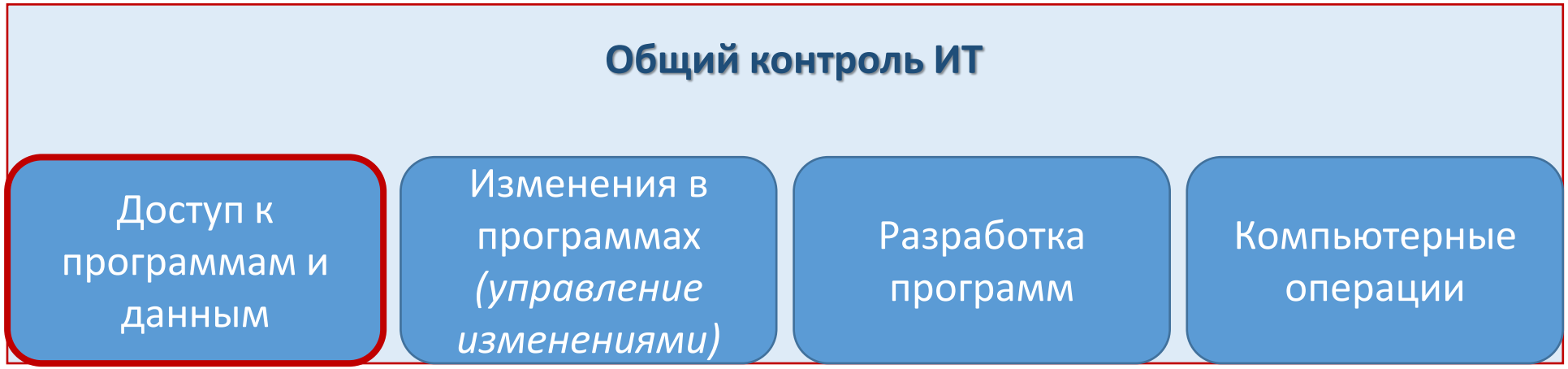
Общие средства контроля информационно-технологических систем *(ОСКИТ)*

Пример

Обзор общих средств контроля ИТ – процесс аудита

- Понять и определить подлежащие рассмотрению ИТ—среду и ИТ-системы
- Провести собеседование, пошаговый разбор и проанализировать документацию для формирования понимания технологических процессов
- Понять и определить подлежащие рассмотрению ИТ—среду и ИТ-системы
- Оценить адекватность существующей контрольной среды (структуры контроля)
- Проверить существующие средства контроля для оценки функциональной эффективности контроля

Обзор общих средств контроля ИТ – Доступ к программам и данным



Цели:

Доступ к программам и данным надлежащим образом ограничен и предоставлен исключительно лицам, имеющим допуск.

Риск:

Несанкционированный доступ к программам и данным может привести к неправомерному изменению данных или их уничтожению.

Обзор общих средств контроля ИТ – Доступ к программам и данным

Необходимо рассмотреть вопросы доступа к следующим компонентам программ и данных:

- Политика и процедуры
- Предоставление и отключение доступа для пользователей
- Периодические обзоры доступа
- Требования к паролю
- Управление привилегированными учетными записями пользователей
- Физический доступ
- Соответствие доступа кругу полномочий
- Аутентификация системой
- Журналы аудита

Обзор общих средств контроля ИТ – Доступ к программам и данным, пример

Направление	Существующая структура средства контроля	Как протестировать/проверить
Предоставление доступа пользователю	Действует официальный процесс предоставления или изменения доступа к системе (на основе соответствующего уровня согласования).	Рассмотреть доказательства такого согласования
Лишение пользователя доступа	Действует официальный процесс отключения доступа для переведенных или уволенных пользователей.	Сравнить действующие учетные записи пользователей со списком пользователей, которые
Периодический анализ доступа	Проводятся периодические обзоры доступа пользователей, администраторов и сторонних поставщиков.	Рассмотреть доказательства наличия периодического анализа
Требования к паролям	Используются уникальные (для индивидуального пользователя) и надежные пароли.	Оценить применяемые правила формирования паролей
Привилегированные учетные записи пользователей	Учетные записи с привилегированными правами доступа к системе (например, к серверам, базам данных, приложениям и инфраструктуре), могут иметь только специально уполномоченные сотрудники.	Проверить учетные записи с привилегированными правами доступа
Физический доступ	Доступ в охраняемые зоны и к компьютерному оборудованию разрешен только уполномоченному персоналу..	Физический осмотр помещений (например, центра обработки данных, хранилища резервных копий и т.д.).

Обзор общих средств контроля ИТ – Изменения программ

Цели:

Все изменения действующих систем должным образом санкционируются, проверяются, утверждаются, внедряются и документируются.

Риск:

Ненадлежащие изменения, вносимые в системы или программы, могут привести к неточностям в данных.

Обзор общих средств контроля ИТ – Изменения программ

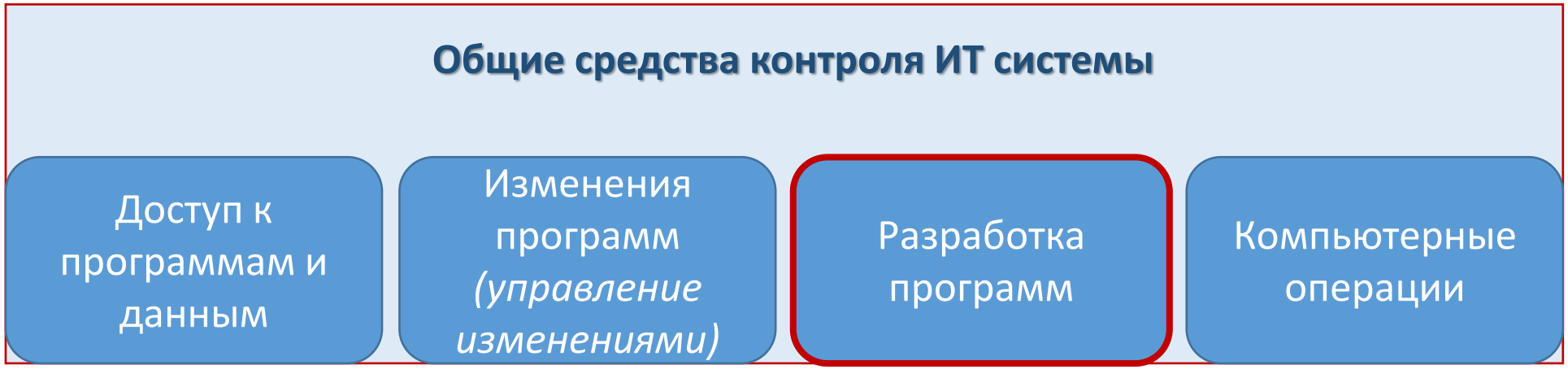
Необходимо рассмотреть следующие изменения программ и компонентов разработки :

- Процедуры управления изменениями и методология разработки систем
- Разрешение, разработка, внедрение, тестирование, утверждение и документирование
- Перенос в производственную среду (Разделение обязанностей (SOD))
- Изменения конфигурации
- Экстренные изменения
- Миграция данных и контроль версий
- Тестирование и обзоры после изменения/внедрения

Обзор общих средств контроля ИТ – Изменения программ, пример

Направление	Существующая структура средства контроля	Как протестировать/проверить
Средства контроля управления изменениями	Действует официальный процесс надлежащего управления изменениями.	Проверить/оценить процедуры управления изменениями и найти подтверждение соблюдению процедур
Документация об изменениях	Все изменения, вносимые в системы (например, серверы, базы данных, приложения, пакетные задания и инфраструктуру), документируются и отслеживаются.	Проверить журналы изменений
Тестирование	Тестирование осуществляется на надлежащем уровне.	Рассмотреть доказательства наличия планов и результатов тестирования
Утверждение	Для переноса в производство необходимо получить соответствующее утверждение.	Проверить наличие доказательства утверждения
Перенос	Доступ к возможности переноса изменений в производство надлежащим образом ограничен.	Убедиться, что существует разделение обязанностей (SOD) между разработчиками и операторами (= внесению изменений).

Обзор общих средств контроля ИТ – разработка программ



Цели:

Разрабатываемые или внедряемые новые системы/приложения должным образом санкционированы, испытаны, утверждены, внедрены и задокументированы.

Риск:

Ненадлежащая разработка или внедрение системы или программы может привести к неточности данных, финансовым потерям и т.д.

Обзор общих средств контроля ИТ – разработка программ

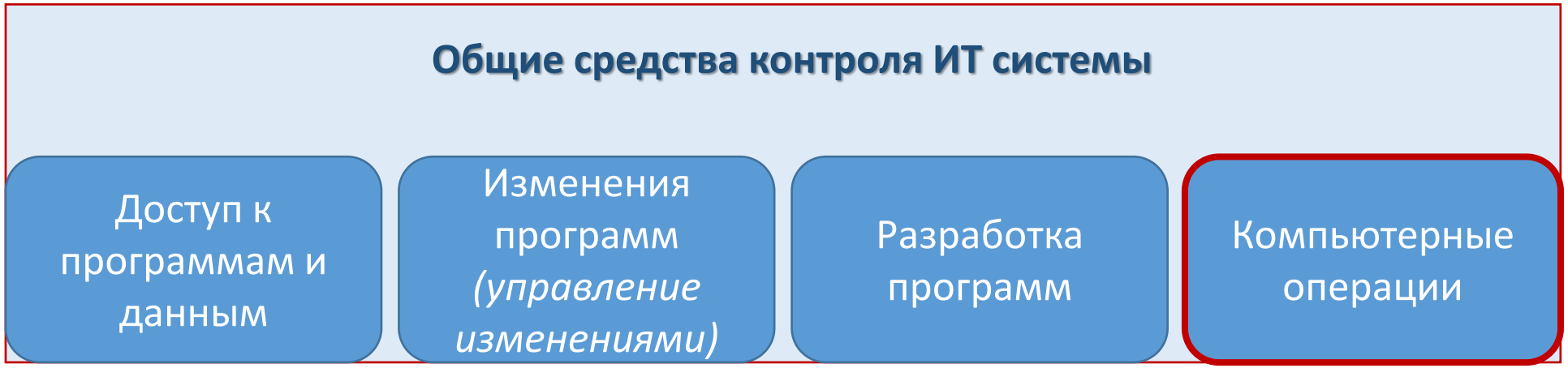
Подлежащие рассмотрению компоненты разработки программ:

- Требования к пользователю, ТЗ
- Разработка
- Конфигурация/код
- Тестирование
- Внедрение
- Оценка
- Поддержка

Обзор общих средств контроля ИТ – ЦРПО, пример

Направление	Структура существующего средства контроля	Как протестировать/проверить
Требования к пользователю	Существует документально оформленный процесс утверждения требований к пользователю.	Проверить и убедиться в наличии документально оформленных и утвержденных требований к пользователю.
Разработка и кодирование	????	????
Тестирование	????	????
Внедрение	????	????
Оценка и приемка	????	????
Поддержка	????	????

Обзор общих средств контроля ИТ – компьютерные операции



Цели:

Системы и программы имеются в наличии и работают с высокой точностью

Риск:

Системы или программы могут быть недоступны для пользователей или работать неточно.

Обзор общих средств контроля ИТ – компьютерные операции

Необходимо рассмотреть следующие компоненты компьютерных операций:

- Обработка пакетных заданий
- Мониторинг выполнения заданий (успех/неудача)
- Процедуры резервного копирования и восстановления
- Работа с инцидентами и устранение проблем
- Изменения в графиках выполнения пакетных заданий
- Средства контроля для предотвращения утечки информации
- План послеаварийного восстановления (ПАВ) и План обеспечения непрерывности бизнеса (ПОНБ)
- Управление корректирующими вставками

Обзор общих средств контроля ИТ – компьютерные операции, пример

Направление	Структура существующего средства контроля	Как протестировать/проверить
Обработка пакетных заданий	Пакетные задания должным образом планируются, обрабатываются, контролируются и отслеживаются.	Проанализировать/оценить процедуры обработки и контроля пакетных заданий и убедиться в соблюдении этих процедур.
Мониторинг выполнения заданий	Обеспечивается последующий контроль и документирование случаев невыполнения заданий (включая успешное решение и пояснения).	Убедиться в том, что невыполненные задания отслеживаются и документируются.
Резервное копирование и восстановление	На случай чрезвычайной ситуации имеются резервные копии критически важных данных и программ.	Проанализировать/оценить процедуры резервного копирования и восстановления и убедиться в их соблюдении.
Управление неисправностями/проблемами	Для обеспечения своевременного выявления, эскалации, решения и документирования проблемы предусмотрен официальный процесс ее урегулирования.	Проанализировать/оценить процедуры урегулирования проблем и убедиться в их соблюдении

Вопросы


Thank You