



Ukraine

Вище надійність.
Більше цінність.

www.tuv-sud.com.ua

Сравнительный анализ стандартов ISO/IEC 27001 и ISO/IEC 20000-1

Ильдар Гарипов



Ukraine



ISO/IEC 27001



ISO/IEC 20000-1

Заданные величины четко определены и последовательны
действуют на всех уровнях

Сплошной
Контроль

ИТ-услуги

Более высокая
эффективность

Постоянное
улучшение

Процессы приводятся в
оптимальное соответствие с
потребностями

Не все сразу становится отличным,
но все делается для того, чтобы
сделать это лучше

Система менеджмента

PDCA

**Ответственность
руководства**

Документация

**Анализ со
стороны
руковод-**

**Внутренний
аудит**

Производственные процессы

Внедрение новых услуг

**Процессы предоставления
услуг**

**Процессы
утверждения**

**Процессы
контроля**

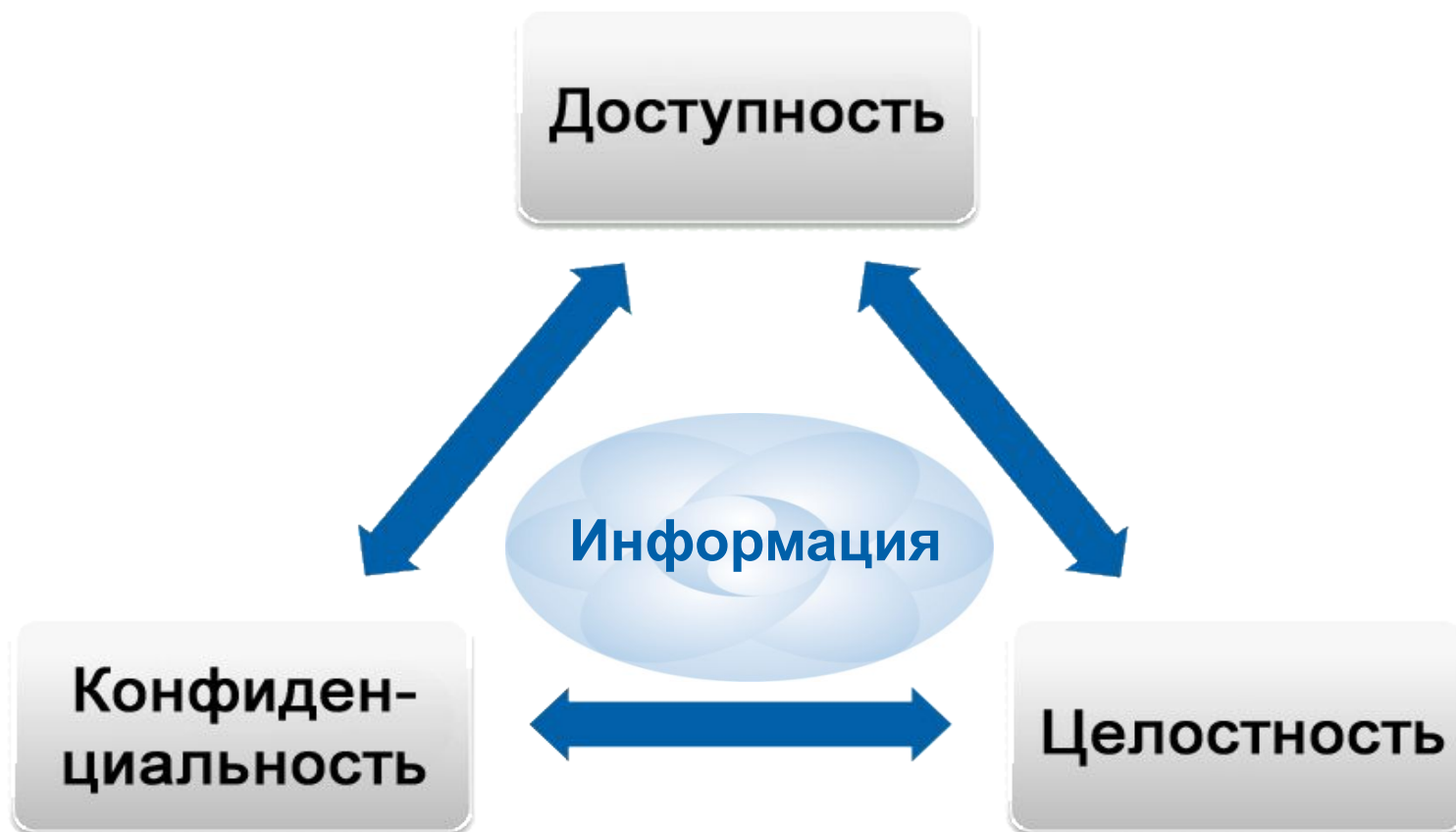
**Процессы
решения**

**Процессы
отношений**

Система менеджмента основывается на базисной концепции ISO 9001

Специальные аспекты ISO 20000, опирающиеся на ITIL®

Важная для бизнеса информация
доступна, когда вы в ней нуждаетесь

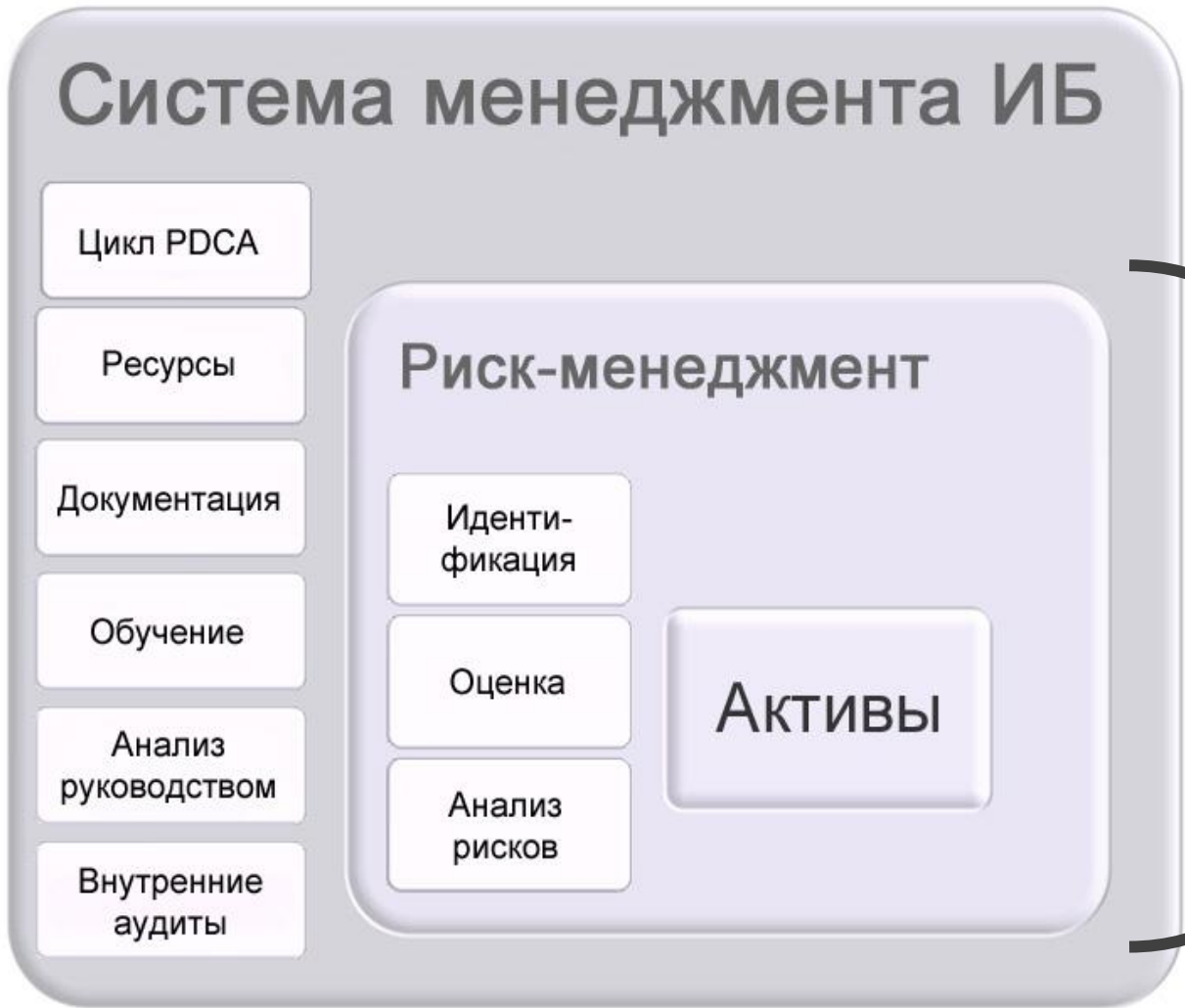


Только уполномоченные лица
получают доступ к информации

Информация в полном объеме и
достоверная



Ukraine



Система менеджмента основана на процессном подходе (ISO 9001)

Важнейший инструмент стандарта ISO 27001



Ukraine

Разработка и преобразование новых или измененных сервисов

Процессы предоставления сервисов

Управление мощностями

Управление уровнем сервиса

Управление
информационной
безопасностью

Управление непрерывностью
и доступностью

Отчетность по предоставлению
сервиса

Бюджетирование и
учет затрат

Процессы контроля

Управление конфигурациями

Управление изменениями

Управление релизами и
развертыванием

Процессы разрешения

Управление проблемами

Управление инцидентами и запросами

Процессы управления взаимоотношениями

Управление взаимоотношением с
бизнесом

Процессы предоставления сервисов

Приложение А. (Обязательное)

A.5 Политика в области безопасности

A.6 Организация системы безопасности

A.7 Классификация активов и управление

A.8
Безопасность
и персонал

A.9
Физическая и
внешняя
безопасность

A.10
Менеджмент
компьютеров
и сетей

A.12 Приобретение,
разработка и
обслуживание
информационной
системы



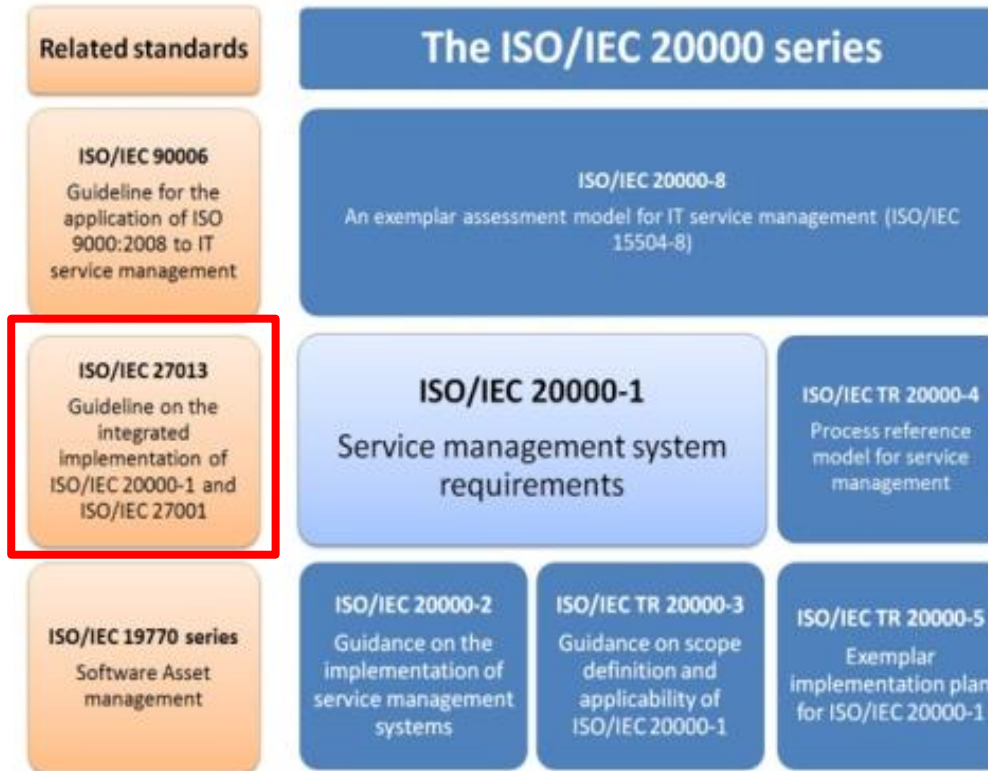
A.11 Управление доступом к системе

A.13 Менеджмент инцидентов информационной безопасности

A.14 Обеспечение непрерывности бизнеса

A.15 Соответствие законодательству

ISO/IEC 27013 — "IT Security — Security techniques — Guideline on the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001"





Ukraine

Управление изменениями

ISO 20k (9.2): гарантировать, что все изменения оценены, утверждены, осуществлены и проанализированы посредством реализации принятых методов и процедур, обеспечивающих их своевременную и результативную обработку

ISO 27k (A.10.1.2): изменения в системах и средствах обработки информации необходимо контролировать.



Ukraine

Процессы предоставления сервисов

ISO 20k (7.2): управлять подрядчиками для обеспечения качества сервисов

ISO 27k (A.10.2): реализовать и поддерживать подходящий уровень защиты информации предоставления сервисов.



Ukraine

Управление мощностями

ISO 20k (6.5): гарантировать, что поставщик сервисов имеет мощности, достаточные для удовлетворения текущих и будущих потребностей бизнеса

ISO 27k (A.10.3.1): использование ресурсов должно постоянно контролироваться, регулироваться, и должны делаться прогнозы будущих требований производительности, чтобы гарантировать требуемые характеристики работы системы.



Ukraine

Разработка и преобразование новых или измененных сервисов

ISO 20k (5): гарантировать, что новые и измененные услуги будут предоставляться и управляться в соответствии с согласованными затратами и установленным качеством

ISO 27k (A.12): гарантировать, что защита является неотъемлемой частью информационных систем



Ukraine

Управление инцидентами и запросами

ISO 20k (8; 6.6.3): как можно быстрее восстановить предоставление сервиса и минимизировать отрицательное влияние инцидентов на бизнес

ISO 27k (A.13.2): гарантировать применение последовательного и результативного подхода к менеджменту инцидентов в системе защиты информации.



Ukraine

Управление непрерывностью и доступностью сервисов

ISO 20k (6.3): гарантировать, что согласованные обязательства по непрерывности и доступности будут выполнены при любых обстоятельствах

ISO 27k (A.14): противодействовать прерываниям в деловых операциях, защитить деловые процессы от влияния существенных сбоев информационных систем или бедствий, а также гарантировать своевременное возобновление деловых операций

Управление информационной безопасностью

ISO 20k (6.6) - ISO 27k (A.10; A11;A12): эффективно управлять информационной безопасностью при предоставлении сервисов





Ukraine

Большое спасибо за внимание

www.tuv-sud.com.ua

Ильдар Гарипов

Ildar.Garipov@tuv-sud.com.ua

