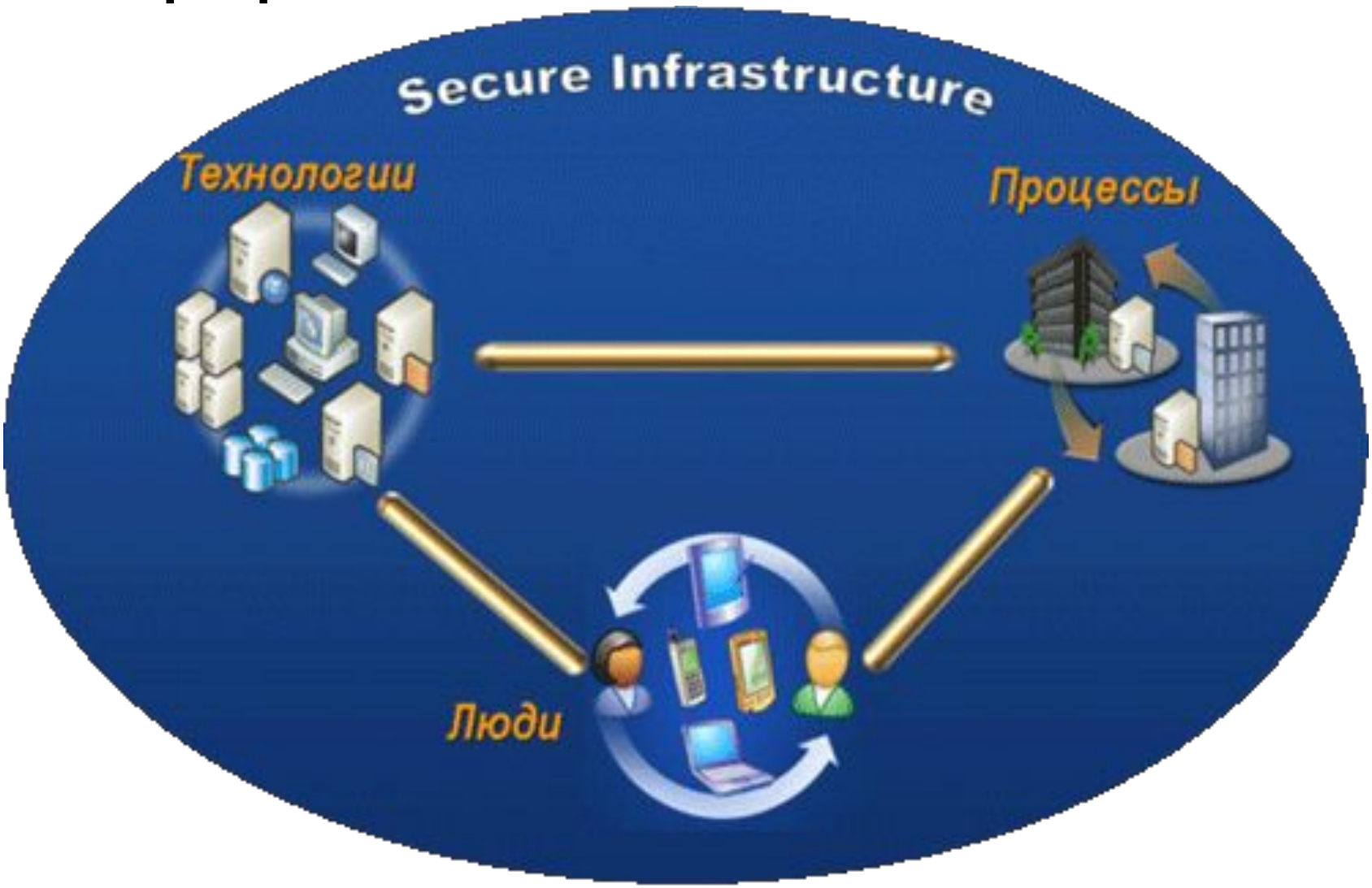
Информационная безопасность

Ключевые компоненты информационной безопасности



Уязвимости технологий:

– отсутствие определенных функций безопасности,
– бреши и ошибки в продуктах,
– трудности с обеспечением взаимодействия между компонентами,
– Элементы технологий, не соответствующие стандартам.

«Человеческий фактор"

- некомпетентность,
- непрофессионализм,
- отсутствие опыта,
- шантаж,
- подкуп.

- Процессы должны обеспечивать эффективное взаимодействие технологий и людей, в том числе они должны обеспечивать создание безопасной ИТ-инфраструктуры.

Подход Microsoft к обеспечению ИТ-безопасности

- Конфиденциальность - каждый пользователь должен сам управлять своими документами и правами на осуществление тех или иных действий с ними.

- Надежность подразумевает, что пользователь может получить доступ к ресурсам при необходимости, а также должен быть уверен в работоспособности ожидаемого уровня.

- Бизнес-интеграция - это, помощь пользователям в поиске требуемых решений.

Оценка безопасности

Модель угроз и процесс обеспечения ИТ-безопасности

- Эффективное решение безопасности возможно тогда и только тогда, когда реальные риски идентифицированы, а их воздействие оценено.


Доступность
Как повлияет отключение или недоступность систем?
Целостность
Каковы последствия искажения или фальсификации информации?
Доверие
Доверяют ли пользователи информации?
Конфиденциальность
К чему приведёт неавторизованное распространение информации?

Текущее состояние

Доказательство

Какой специфический измеряемый критерий указывает на существование проблемы? (например, хакерские атаки, «хвосты» или следы проникновения)

Влияние

Что будет в случае постоянного существования этой проблемы? (например, потеря заказчиков, информации…)

Будущее состояние

Доказательство

Как будет измеряться успех любого предложенного решения? (например, уменьшение брешей безопасности)

Влияние

Что будет максимальным вознаграждением если решение заработает? (например, снижение финансовых потерь вследствие краж информации)

Области в которых необходимо проводить оценку рисков

Область	Описание
Ключевые бизнес-процессы	Администрирование, аутентификация, контроль доступа, критически важные приложения
Модель администрирования	Централизованная или распределённая, размещение ИТ-специалистов, использование «внешних» специалистов и их функции, критерии делегирования ИТ-ответственности
Схема организации пользователей	Требования к конечным пользователям, профили групп пользователей, требования департаментов и сайтов, профили удалённых пользователей
Информационная архитектура	Документопотоки, расположение хранилищ данных
Технологическая архитектура	Физическая топология, логическая топология, инфраструктура Active Directory™, инфраструктура безопасности
IT и другие стандарты	Организационные, технологические, безопасности

Варианты изменения рисков IT-безопасности

- Устранение, риск полностью нейтрализуется навсегда. Например, была выявлена уязвимость, которая полностью исчезает после установки соответствующих исправлений.

  Ослабление - устранение невозможно или нереально технологически или экономически, ослабление помогает снизить риск на соответствующих уровнях. В качестве ослабляющих риск мер можно предложить административные ограничения, охватывающие те или иные зоны.

  Управление - если риск не может быть устранён или ослаблен, остаётся лишь управлять риском (например, за счёт страхования). Следует отметить, что управлять риском удается далеко не всегда.

  Исключение - когда нет других доступных вариантов, и воздействие угрозы слишком велико для продолжения функционирования, организации могут предпочесть демонтировать и/или реконструировать систему(-ы).