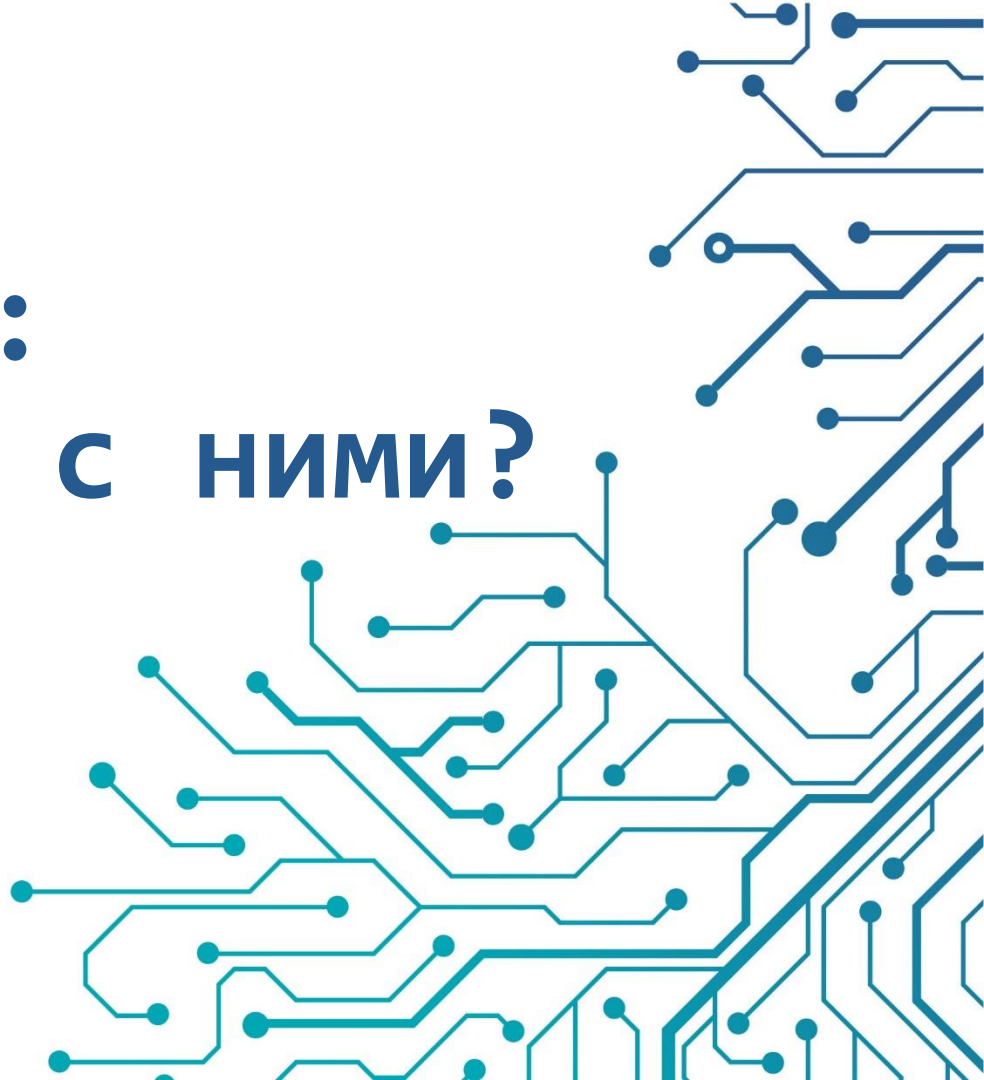
Требования безопасности: как работать с ними?

Жигулина Александра
Ведущий системный аналитик



infotecs

О себе

- 7 лет работы бизнес и системным аналитиком
- 5 лет работы в компании-производителе средств защиты информации «ИнфоТеКС» в роли системного аналитика
- 3 года в роли тимлида команды аналитиков в отделе криптографии «ИнфоТеКС»
- Текущая деятельность: требования для криптографических библиотек, форматов и протоколов VPN

План презентации

- Понятие безопасности
- Какие трудности могут быть при выявлении и анализе требований безопасности
- Подход 1: опираемся на законы и стандарты
- Подход 2: используем модели угроз и защиты
- Подход 3: затыкаем дыры (импровизируем)
- Какие умения мы получим?

ПОНЯТИЕ БЕЗОПАСНОСТИ

Понятие безопасности в целом

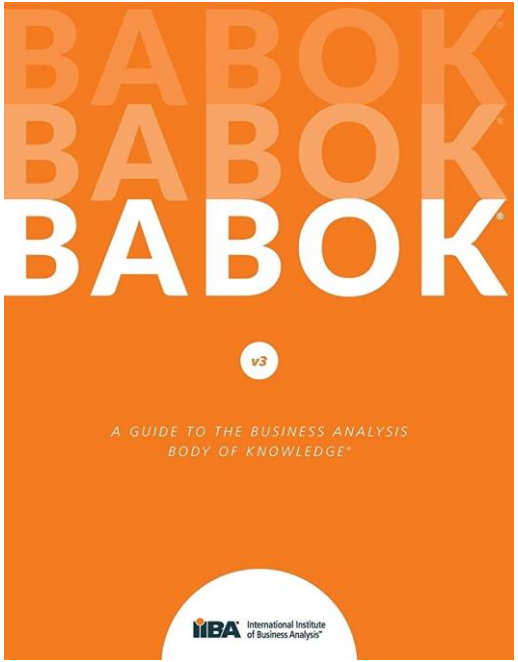
Безопасность – состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз ФЗ «О безопасности»

Безопасность информации – деятельность, направленная на предотвращение или существенное затруднение несанкционированного доступа к информации (или воздействия на информацию) ФСТЭК

Категории нефункциональных требований

Безопасность – аспекты решения, защищающие содержимое или компоненты решения от случайного или злонамеренного доступа, использования, разрушения или раскрытия

Доступность – степень, в которой решение является работоспособным и доступным, когда это требуется для использования, при этом часто выражается в процентах времени, в течение которого решение доступно



ТРУДНОСТИ ВЫЯВЛЕНИЯ И АНАЛИЗА ТРЕБОВАНИЙ БЕЗОПАСНОСТИ

Стейкхолдеры ИБ

Внутри предприятия:

- ИТ
- ИБ
- Юристы
- Бизнес-подразделения
- Руководство
- Пользователи
- …

Снаружи предприятия:

- Акционеры
- Клиенты
- Партнеры
- Аудиторы
- …

Регуляторы:

- ФСТЭК
- ФСБ
- Роскомнадзор
- PCI Council (PCI DSS)
- ЕС (GDPR)
- …

Руководство

Сделайте безопасно! Вы же знаете как, да?..

Да что вам надо то??

Пользователь

А можно без пароля логиниться?

Регулятор

В законе всё написано!

Ну нет, слишком долго и дорого

Руководство

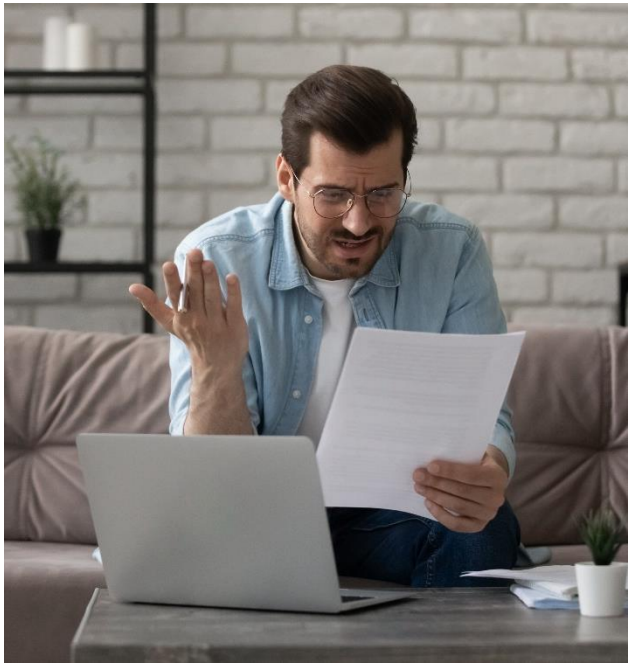
Система

Я так не работаю!

У нас регламенты!

Служба ИБ

Трудности: требования регулятора



- Слишком абстрактны
- Допускают несколько вариантов решения
- Не применимы к конкретной системе или сценарию
- Недостаточны или избыточны для реальной (не бумажной) безопасности у заказчика

Пример: для всех пользователей системы должна быть реализована двухфакторная аутентификация

Трудности: требования заказчика

- «Кусочные» требования к безопасности решения
- Свойства безопасности бывают разные, как расставить приоритеты?

Трудности: требования заказчика

- Требования к безопасности противоречат другим требованиям или ожидаемой стоимости решения
- А зачем нам вообще эта безопасность?
- Когда остановиться в формулировании требований к безопасности и как избежать паранойи?

Пример: пользователь должен получать полный доступ к функциям приложения за один шаг

Трудности: другие НФТ

Соответствие
Сертификация
Совместимость
Переносимость
Локализация
Расширяемость
Доступность
Удобство
Масштабируемость
Надёжность
Эффективность
Ремонтопригодность
Производительность
Соглашения об уровне обслуживания

Обычно мешает
Чаще мешает, чем помогает
Не влияет или двояко
Обычно помогает

Трудности: устройство системы

- Проектировалась без учёта требований безопасности
- Меры защиты делают систему неработоспособной или бесполезной
- Известные подходы к безопасности неприменимы к системе нестандартного типа

Пример: устройство не имеет физического интерфейса для ввода второго фактора аутентификации

Трудности: предубеждения аналитика

- Безопасность это абстракция, с которой непонятно как работать (поэтому и не будем)
- В безопасности разбираются только эксперты, самому даже и пытаться не стоит. Как скажут эксперты – так и сделаем
- Мы сначала запилим функционал, а потом уже безопасники скажут что доделать
- Заказчик не просил безопасное решение, значит пока не нужно

ПОДХОД 1: ОПИРАЕМСЯ НА ЗАКОНЫ И СТАНДАРТЫ

Требования регулятора или стандарты

План действий:

- Собрать информацию из руководящих документов и стандартов
- Отсеять лишнее, оставить обязательные требования, а также стандарты, которые кажутся полезными
- Подумать, как применить в конкретной системе

Откуда взять:

- Российские – ФСБ, ФСТЭК.. См. обзор Лукацкого
- Зарубежные – NIST, FIPS, BSI, PCI DSS, ISO..

Пример про аутентификацию

- Требование ФСБ: для всех пользователей системы должна быть реализована двухфакторная аутентификация
- Стандарт NIST Special Publication 800-63B:
  - пароли желательно проверять на стойкость, например исключать пароли из повторяющихся символов, пароли совпадающие с логином, пароли из известных утечек
  - В аутентифицирующем устройстве нежелательно хранить секретные данные, которые могут быть скомпрометированы и использованы нарушителем для аутентификации на том же устройстве
  - …

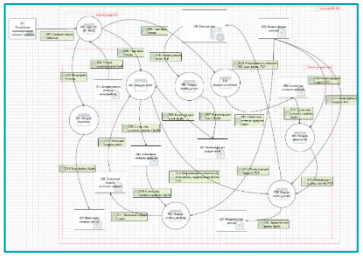
Требования регулятора или стандарты

- ✓ Выполнили законы и отраслевые стандарты
- ✓ Поняли, от чего оттолкнуться, если изначально информации было недостаточно
- ✓ Узнали мнение экспертов в безопасности и лучшие практики

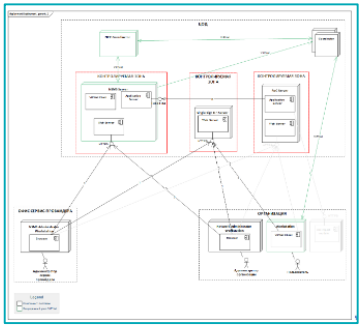
- × Как оптимально применить требования и практики в конкретной ситуации?
- × Как обосновать перед заказчиком применение необязательных рекомендаций?
- × Очень много читать, не факт что найдёшь нужное
- × А если у нас нет требований регулятора и подходящих стандартов?

ПОДХОД 2: ИСПОЛЬЗУЕМ МОДЕЛИ УГРОЗ И ЗАЩИТЫ

Модель угроз и модель защиты



Модель угроз (что плохого может произойти?) – физическое, математическое, описательное представление свойств и характеристик угроз безопасности информации ГОСТ 50922-2006



Модель защиты (как мы планируем защититься?) – абстрактное (формализованное или неформализованное) описание комплекса программно-технических средств и (или) организационных мер защиты от несанкционированного доступа Приказ председателя Гостехкомиссии России от 30.03.1992 «Защита от несанкционированного доступа к информации. Термины и определения»

Посмотреть модель угроз

Из модели угроз выяснить:

- В каких местах система может быть атакована
- Какие атаки есть смысл рассматривать
- Каких нарушителей есть смысл рассматривать

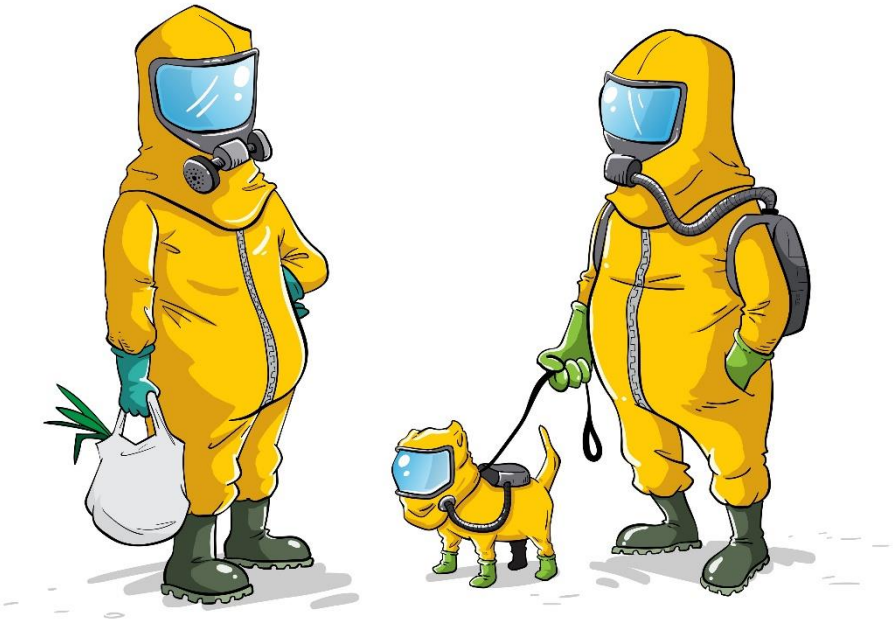
Посмотреть модель угроз

Из модели угроз выяснить:

- Приоритет требований безопасности, по величине риска
- Максимальные разумные затраты на закрытие уязвимости

Риск = Величина ущерба × Вероятность возникновения

Посмотреть модель защиты



- Из модели защиты выяснить:
  - Какие требования безопасности уже закрыты тем или иным способом, или как уже ранее решено их закрывать
- Не принимать всё на веру!

Найти модели угроз и защиты

- Часто уже есть
  по требованиям регулятора для:
  - ГИС
  - Система обработки персональных данных
  - КИИ
  - СЗИ/СКЗИ
  - Практики безопасной разработки в компании
- Или сделать самому

Пример про аутентификацию

- **Из модели угроз узнали, что:** в одном из сценариев пароль пользователя передаётся по сети в открытом виде
- **Решение:** либо отказаться от поддержки сценария, либо передавать пароль по защищённому соединению с шифрованием

Посмотреть модель угроз

- ✓ Рассмотрели систему как целое, узнали весь список угроз, включая неочевидные
- ✓ Требования безопасности чётко обоснованы и приоритизированы выявленными рисками

- × Модели угроз нет, и нет времени её сделать
- × Модель угроз недостаточно подробна для ответа на конкретный вопрос

ПОДХОД 3: ЗАТЫКАЕМ ДЫРЫ (ИМПРОВИЗИРУЕМ)

Затыкание дыр: дисклеймер

При повсеместном использовании ведёт к бессистемному решению только части проблем

НО:

- А если решение нужно срочно, а модели угроз нет?
- А если модель угроз не идеальна?
- А если ответ на вопрос требует дополнительных логических рассуждений с опорой на модель угроз?

Какое свойство безопасности требуется?

Для информации:

- **Конфиденциальность**
- **Целостность**
- **Доступность**
- Подлинность (аутентичность)
- Неотказуемость…

Пример: доступ к перечисленным функциям системы должны иметь только администраторы – значит пользователи должны быть аутентифицированы

Какое свойство безопасности требуется?

Для физического объекта:

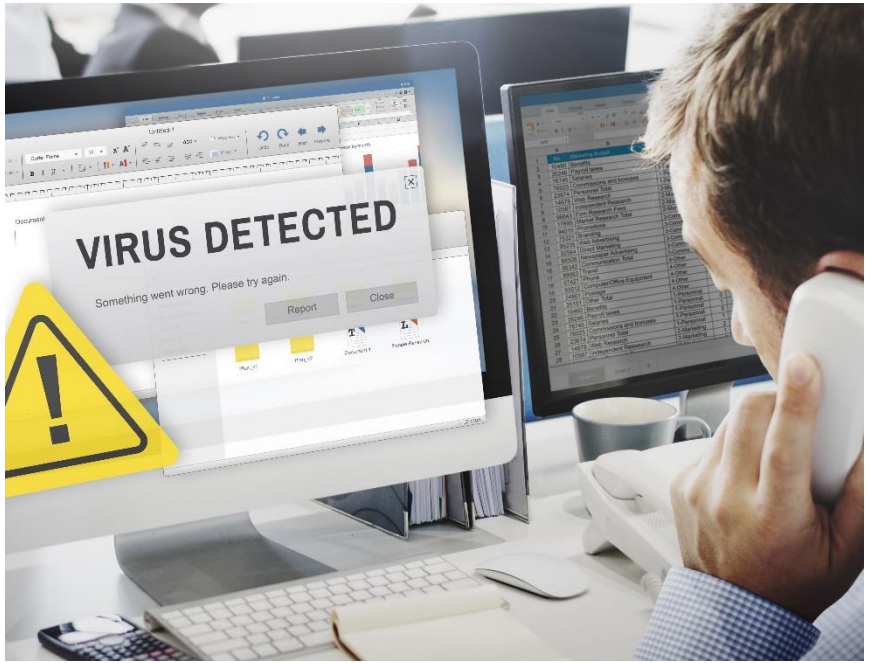
- Защиты от кражи
- Удержание контроля
- Исправность
- …

Какое свойство безопасности требуется?

Для людей:

- Здоровье
- Предупреждение увольнения
- …

Какие проблемы с безопасностью были в прошлом у нас?



- Утечка персональных данных
- Утечка паролей
- DDoS атака на сайт
- Повреждение критичных файлов
- Заражение компьютера зам. директора…

Пример: нарушитель подобрал слабый пароль к учётке пользователя и совершил противозаконные действия

Какие пользовательские сценарии у нарушителя?

- Какой нарушитель соответствуют предполагаемому сценарию атаки?
- А есть ли у нас такой нарушитель, который может провести данную атаку?
- Какая цепочка действий будет у конкретного типа нарушителя в конкретном сценарии?

Типовые нарушители

Источник: http://crypto-anarchist.blogspot.com/2015/07/blog-post.html

ПП 1119	Приказ ФСТЭК №17	Проект методики определения угроз ФСТЭК		Методические рекомендации ФСБ по моделированию угроз	Метод. рек. ФСБ 2008	Приказ ФСБ 378
Тип угроз	Класс ГИС и соотв. набор мер	Потенциал нарушителя	Вид нарушителя	Обобщенные возможности нарушителя относительно СКЗИ	Тип нарушителя ФСБ	Класс СКЗИ
3 тип	К3, К4	Низкий	Внешние субъекты (физические лица)	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны	Н1	КС1
			Бывшие работники (пользователи)			
			Лица, обеспечивающие функционирование информационных систем или обслуживающих инфраструктуру оператора	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам (далее – АС), на которых реализованы СКЗИ и среда их функционирования	Н2	КС2
			Лица, привлекаемые для установки, наладки, монтажа, пуско-наладочных и иных работ	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к АС, на которых реализованы СКЗИ и среда их функционирования	Н3	КС3
			Пользователи информационной системы			
2 тип	К2	Средний	Администраторы информационной системы и администраторы безопасности	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области анализа сигналов линейной передачи и сигналов побочного электромагнитного излучения и наводок СКЗИ)	Н4	КВ
			Преступные группы (криминальные структуры)	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей прикладного программного обеспечения)	Н5	
			Конкурирующие организации			
			Разработчики, производители, поставщики программных, технических и программно-технических средств			
1 тип	К1	Высокий	Специальные службы иностранных государств (блоков государств)	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей аппаратного и программного компонентов среды функционирования СКЗИ)	Н6	КА

Пример про аутентификацию

- Вопрос: может ли кто-то подменить данные в системе так, чтобы система аутентифицировала нелегальных пользователей?
- Нарушитель: имеет доступ к физическому устройству с данными для аутентификации пользователя, иначе не смог бы провести атаку
- Что ещё может такой нарушитель:
  - Подменить все остальные файлы на устройстве – с помощью стандартных средств ОС или путём замены блока памяти
  - Подменить резервные копии с данными для аутентификации…
- Аутентифицировать нелегальных пользователей можно и без подмены данных в системе

Что будет, если не выполнить требование безопасности?

- Денежные потери
- Репутационные потери
- Потеря лояльности клиентов
- Потеря доли рынки
- Ничего не будет?...

Пример: неаутентифицированный пользователь (злоумышленник) с правами администратора может вывести интернет-магазин из строя на значительное время. Это приведёт к прямым денежным потерям из-за того, что пользователи не смогут ничего купить на сайте.

Результат «затыкания дыр»

- ✓ Быстрое принятие решения в конкретной ситуации
- ✓ Выяснили настоящую потребность в безопасности за хотелкой заказчика
- ✓ Перепроверили предыдущие решения, включая модель угроз

- × Решению может недоставать полноты, риск «кусочного» решения проблемы
- × Возможно упущено более общее решение проблемы на основе существующих стандартов и методических рекомендаций

Какие умения мы получим?

Какие умения мы получим?

- Иметь обоснованную позицию в части требований безопасности к разрабатываемой системе
- Критически воспринимать советы экспертов по безопасности и хотелки заказчиков
- Находить компромисс с другими типами требований

Спасибо за внимание!

Жигулина Александра

Ведущий системный аналитик

e-mail: Aleksandra.Zhigulina@infotecs.ru

Подписывайтесь на наши соцсети

vk.com/infotecs_news

t.me/infotecs_news

rutube.ru/channel/24686363

Шпаргалка по BABOK

- **Доступность:** степень, в которой решение является работоспособным и доступным, когда это требуется для использования, при этом часто выражается в процентах времени, в течение которого решение доступно.
- **Совместимость:** степень успешности взаимодействия решения с другими компонентами своего окружения, например, взаимодействия одного процесса с другим.
- **Функциональность:** степень соответствия функций решения потребностям пользователей, включая такие аспекты, как пригодность, точность, совместимость.
- **Ремонтопригодность:** легкость изменения решения или компонента для исправления ошибок, улучшения производительности или других атрибутов, либо для адаптации к изменениям окружения.
- **Эффективность работы:** способность решения или компонента выполнять свои целевые функции с минимальным потреблением ресурсов. Может определяться исходя из контекста или периода, например, пиковое, среднее и минимальное использование.
- **Переносимость:** легкость переноса решения или компонента из одной среды в другую.
- **Надежность:** способность решения или компонента выполнять требуемые функции в определенных условиях в течение определенного периода времени, например, среднее время работы устройства до сбоя.
- **Масштабируемость:** способность решения расти или развиваться, чтобы справиться с растущими объемами работы.
- **Удобство использования:** легкость, с которой пользователь может научиться использовать решение.
- **Сертификация:** ограничения решения, которые необходимо удовлетворить для соответствия неким стандартам или отраслевым соглашениям.
- **Соответствие:** нормативные, финансовые или правовые ограничения, которые могут варьироваться в зависимости от контекста или юрисдикции.
- **Локализация:** требования, касающиеся местных языков, законов, валют, культур, правописания и других характеристик пользователей, требующих внимания к контексту.
- **Соглашения об уровне обслуживания:** ограничения обслуживаемой решением организации, официально утвержденные как поставщиком, так и пользователем решения.
- **Расширяемость:** способность решения включать новую функциональность.