Как выполнить требования ИБ, поступающие из многих независимых источников (включая PCI DSS)

А.Н.Велигура, CISA

Председатель Комитета по банковской безопасности

Ассоциации российских банков

Как выполнить?

Сначала их нужно увидеть…

Источники

Федеральные законы, постановления правительства

Документы ФСБ, ФСТЭК, Роскомнадзора

Требования Банка России

Прочие (например, PCI DSS)

Внутренние нормативные документы организации

Обычные действия

Новые требования документируются

Вносятся изменения в систему мер и средств обеспечения ИБ

Результат (после ряда итераций)

Труднообозримый набор внутренних документов, с дублированием, лакунами и несоответствиями

+

отсутствие уверенности, что ничего не пропущено

Мечты (высказанные в личных беседах)

Во-первых, иметь полный и актуальный список требований по ИБ из всех источников…

Мечты (высказанные в личных беседах)

Во-первых, иметь полный и актуальный список требований по ИБ из всех источников…

Мечты (высказанные в личных беседах)

Во-вторых, уложить их в удобную как для предъявления, так и для использования систему внутренних нормативных документов

Сколько их должно быть?

Пример выполнения

Стандарт СТО БР ИББС 1.0 – попытка изложить основные требования ИБ (и даже более) в одном документе.

Неизбежный результат – плата за универсальность – обобщенность, отсюда необходимость адаптировать положения стандарта для конкретной организации.

Имеется запрос на дополнительные руководства и методические рекомендации по применению стандарта.

Другой пример

Для конкретной организации был определен список основных ВНД + законодательные и прочие требования

и предложено уложить все в 2 документа.

Как увидеть все требования?

Все требования были рассортированы по направлениям обеспечения ИБ. Перечень направлений определяется экспертным методом (например, за основу можно взять разделы 7 и 8 СТО БР ИББС 1.0)

Внутри направлений требования упорядочиваются по тем или иным принципам (по строгости, по характеру, по сфере применения и т.п.).

В результате

Получилась база требований (со ссылками).

Это дало возможность изготовить нужные документы, выбирая требования соответствующего уровня и направленности из разделов базы.

Действуя таким образом:

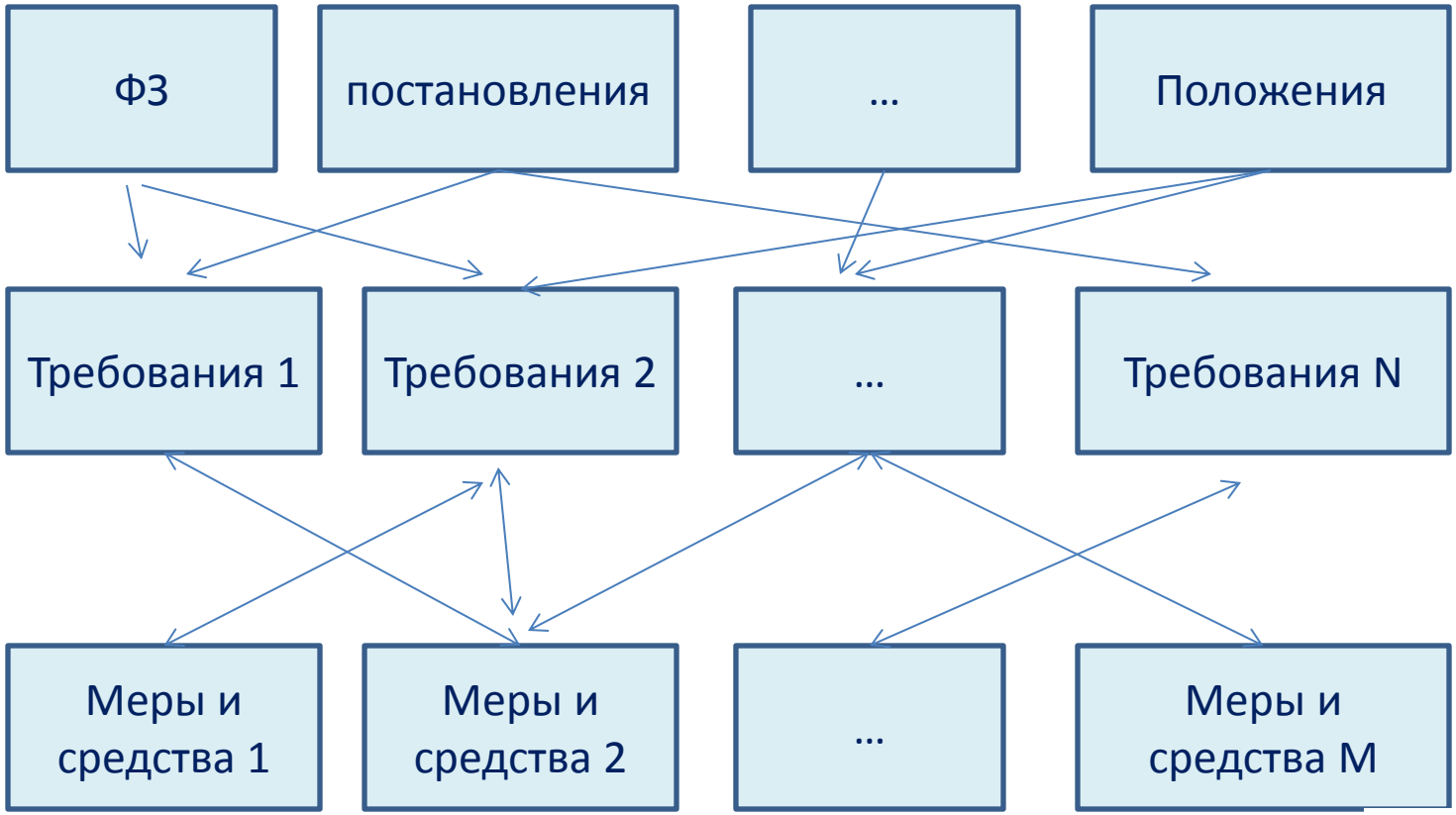
Включение требований легко обосновать.

Дублирования и противоречий проще избежать.

При появлении новых требований или изменений в имеющихся упрощается внесение изменений

Актуализация выполняется путем внесения в базу специфических требований (например, из политики организации или других ВНД).

Следующий шаг – определение мер и средств защиты:



Спасибо за внимание!

Велигура Александр Николаевич

Ассоциация Российских Банков

Председатель комитета
по банковской безопасности
Ассоциации российских банков

Заместитель генерального директора
ООО Андэк Консалтинг

Москва, ул.Городская, д.8
Телефон:+7 (495) 984-60-40
E-mail: a.veligura@andekconsult.ru

АНДЭК КОНСАЛТИНГ