БАЗОВЫЙ УРОВЕНЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОПЕРАТОРОВ СВЯЗИ И ОЦЕНКА УРОВНЯ ЗРЕЛОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОПЕРАТОРА

Кирсанов Виктор

Черствов Тимофей

Система оценки информационной безопасности представляет собой совокупность аппаратно-программных, технических и организационных защитных мер, функционирующих под управлением СМИБ и процессов осознания ИБ, инициирующих и поддерживающих деятельность по менеджменту ИБ.

Назначение СОИБ

В результате проведения оценки ИБ формируется оценка степени соответствия СОИБ эталону, в качестве которого могут быть приняты (в совокупности и отдельно):

- требования законодательства Российской Федерации в области ИБ;
- отраслевые требования по обеспечению ИБ;
- требования нормативных, методических и организационно - распорядительных документов по обеспечению ИБ;
- требования национальных и международных стандартов в области ИБ.

МЕЖДУНАРОДНЫЕ СТАНДАРТЫ

- Рекомендация МСЭ-ТХ.1051-2004 Система управления информационной безопасностью. Требования к телекоммуникациям.
- Рекомендация сектора стандартизаций Международного Союза Электросвязи (МСЭ-Т) Серии X, Приложение 2, «Серии X.800-X849 МСЭ-Т – Приложение по базовому уровню информационной безопасности операторов связи».
- ISO/IEC 27001 - определяет требования к системе менеджмента информационной безопасности.
- ISO/IEC 27002 - содержит свод практики по менеджменту защиты информации.
- ISMF - information Security Management Forum - Форум по менеджменту защиты информации
- O-ISM3 - модель «Open Information Security Management Maturity Model (O-ISM3)», разработана независимым консорциумом The Open Group, полностью учитывает требования ISO / IEC 27000:2009, COBIT, ITIL.
- COBIT 5 for Information Security - методология, которая призвана помочь в решении задачи руководства и управления ИТ на предприятии.

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РФ

- Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ
- Постановление Правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"
- Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
- Приказ ФСБ России от 10 июля 2014 г. N 378 "Об утверждении Состава и содержания организационных технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности"

Требования «Базового уровня»

- Общие рекомендации
- Требования к политикам оператора
- Требования к функциональности
- Требования к взаимодействию

МЕТОДОЛОГИЯ COBIT 5 - ЕДИНЫЙ И ЦЕЛОСТНЫЙ ПОДХОД

- ✓ соответствует новейшим стандартам и подходам, а, следовательно, предприятия могут использовать COBIT 5 в качестве интеграционной методологии для всех подходов к руководству и к управлению.
- ✓ описывает предприятие целиком, предоставляя основу для эффективной интеграции других подходов, стандартов и практических приемов. Единый подход служит целостным источником рекомендаций, написанным технологически независимым, простым языком.
- ✓ обладает простой архитектурой, позволяющей легко структурировать рекомендации в целостный набор публикаций.
- ✓ объединяет знания, ранее размещенные в различных подходах ISACA. Исследуя различные области управления предприятием на протяжении многих лет, ассоциация ISACA разработала ряд подходов и рекомендаций в помощь предприятиям, таких как COBIT, Val IT, Risk IT, BMIS, Board Briefing on IT Governance и ITAF. Методология COBIT 5 интегрирует все эти знания.

COBIT – CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGY (ЗАДАЧИ ИНФОРМАЦИОННЫХ И СМЕЖНЫХ ТЕХНОЛОГИЙ)

Level 0 - Incompleteprocess (Неполный)	Такой процесс еще не внедрен или не способен соответствовать своему назначению. На этом уровне отсутствуют свидетельства систематического достижения процессом своих целей, или таких свидетельств мало.
Level 1 - Performedprocess (Осуществленный)	Процесс внедрен и соответствует своему назначению.
Level 2 - Managedprocess (Управляемый)	Осуществленный процесс предыдущего уровня теперь управляем (то есть планируется, отслеживается и корректируется). Создаются, контролируются и поддерживаются рабочие продукты процесса.
Level 3 - Establishedprocess (Установленный)	Управляемый процесс предыдущего уровня теперь способен получать ожидаемые результаты.
Level 4 - Predictableprocess (Предсказуемый)	Установленный процесс предыдущего уровня теперь получает результаты в условиях заданных ограничений.
Level5 - Optimisingprocess (Оптимизированный)	Предсказуемый процесс предыдущего уровня теперь постоянно совершенствуется, чтобы обеспечивать достижение текущих и будущих целей предприятия.

КОМПЕТЕНЦИИ ЭКСПЕРТОВ ОРГАНА ПО СЕРТИФИКАЦИИ

- могут провести сравнительный анализ функции и процессов информационной безопасности с лидерами отрасли
- определение наиболее уязвимых областей информационной безопасности организации;
- оценку текущего уровня зрелости процессов информационной безопасности и влияние текущего уровня на функционирование организации в дальнейшем;
- разработку программы для повышения уровня зрелости процессов ИБ.
- рекомендации по совершенствованию систему управления информационной безопасности в соответствии с областью деятельности:
- сегмент автоматизированных расчетов с клиентами (биллинг);
  - службы электросвязи;
  - сети передачи данных;
  - ERP-системы;
  - другие.

СПАСИБО ЗА ВНИМАНИЕ

ЧЕРСТВОВ ТИМОФЕЙ
Орган по сертификации средств связи АНО «ЦКС»
Орган по сертификации системы добровольной сертификации «Связь-Эффективность»