

Построение процесса развития и управления ИБ

Петухов Алексей

Лидер центра компетенций
«Кибербезопасность» НТИ Энерджинет,
Руководитель отдела развития продуктов
InfoWatch ARMA

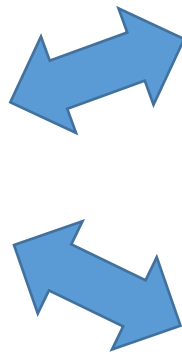


Объект защиты это

Информационная система



Сотрудники



Процессы

Система информационной безопасности

ИСО-МЭК 27001-2013

“Информационные технологии - Методы защиты - Системы менеджмента информационной безопасности - Требования”

- А) Контекст организации
- Б) Лидерство
- В) Планирование
- Г) Обеспечение
- Д) Функционирование
- Е) Оценка результатов деятельности
- Ж) Улучшение



Основан на принципах лидерства, подразумевающих, что высшее руководство компании понимает важность информационной безопасности и систематизирует работу по её управлению

Оценка результатов деятельности

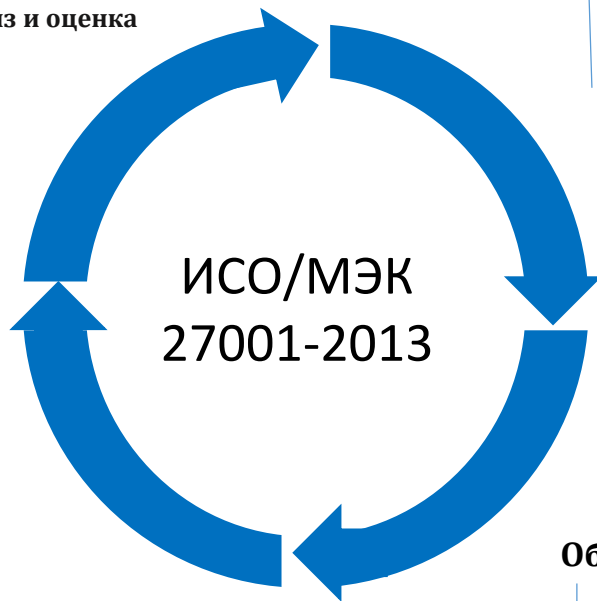
Мониторинг, измерение, анализ и оценка
Внутренний аудит
Анализ менеджмента

Планирование

Цели в области информационной безопасности и планирование их достижения

Действия по обработке рисков и реализации возможностей

+ ФСТЭК 235, 239 для КИИ



Функционирование

Оперативное планирование и управление
Оценка рисков информационной безопасности
Обработка рисков информации

+ ГосСОПКА (ФСБ)

Обеспечение

Ресурсы
Компетентность
Осведомлённость
Коммуникация
Документированная информация

Жизненный цикл ИБ

Модель зрелости процессов в соответствии с требованиями ISO/IEC 21827 «Инжиниринг систем безопасности — модель зрелости возможностей»



	Уровень 1 – Неформальное выполнение:	Уровень 2 - Запланированное и отслеживаемое управление:	Уровень 3 - "Четко Определенный":	Уровень 4 – Количественное управление:	Уровень 5 - Постоянное улучшение:
- РА01 управляет средствами защиты;	+	+	+	+	+
- РА02 оценивает воздействие;		+	+	+	+
- РА03 оценивает риск безопасности;			+	+	+
- РА04 оценивает угрозу;			+	+	+
- РА05 оценивает уязвимость;			+	+	+
- РА06 формирует аргумент доверия;				+	+
- РА07 координирует задачи безопасности;					+
- РА08 проводит мониторинг состояния безопасности;			+	+	+
- РА09 предоставляет входные данные по безопасности;		+	+	+	+
- РА10 обозначает потребности в безопасности;		+	+	+	+
- РА11 проверяет и подтверждает состояние безопасности.		+	+	+	+
- РА12 обеспечивает качество;					+
- РА13 управляет конфигурацией;	+	+	+	+	+
- РА14 управляет проектным риском;		+	+	+	+
- РА15 осуществляет мониторинг и управляет технической деятельностью;			+	+	+
- РА16 планирует техническую деятельность;			+	+	+
- РА17 определяет процесс системного проектирования организации;			+	+	+
- РА18 совершенствует процесс системного проектирования организации;				+	+
- РА19 постоянно обеспечивает практические навыки и знания;				+	+
- РА20 осуществляет сотрудничество с поставщиками.				+	+

**Основные шаги
построения процесса
управления ИБ**



Шаг 1.

Создать рабочую группу с ГД в её руководстве.

Согласовать перечень критичных систем, на которые возможны компьютерные атаки и инциденты, согласованный всеми вовлечёнными руководителями компании.

Шаг 2.

Сформировать актуальные данные и документы для критичных систем:

- Исходные данные по объектам
- Модель угроз и нарушителей
- Целевое проектное решение
- Организационно-распорядительная документация

Далее провести оценку имеющихся ресурсов и сформировать план по их наращиванию до целевого значения, если их недостаточно.

При планировании и оценке рекомендуется сформировать ресурсную матрицу (/таблицу), которая даст представление о том, какие меры реализуются и сколько на каждую из них тратятся ресурсы сейчас и в целевом состоянии.

Шаг 3.

Описать и внедрить процесс управления изменениями:

- Определить перечень изменений, требующих документирования
- Определить формат и сроки фиксации изменений (включая версию)
- Определить ответственных за документацию, а лучше блоки информации в документации (и информационной системе, если такая имеется)
- Сформировать (желательно автоматизированные) процессы документооборота и согласования изменений.

Шаг 4.

Определить ответственных за (под)процессы ИБ и сформировать KPI для них.

Данные метрики должны быть:

- исчисляемы,
- давать качественную и количественную оценки,
- применимы к стадиям жизненного цикла (проектирование, внедрение, эксплуатация, улучшение).

*Должно быть сформировано целевое состояние защищённости

Пример.

Количественные КРІ

- Количество написанных ОРД из общего числа необходимых документов
- Количество сотрудников, прошедших обучение, из общего числа сотрудников, работающих с АСУ
- Частота проверки актуальных угроз по отношению к целевому состоянию
- % технической оснащённости от целевого состояния
- Количество проведённых тренировок

Качественные КРІ

- Время реакции на инциденты по отношению к целевому
- Усреднённый процент применение ОРД в процессах компании
- Средний бал по итогам обучения
- Оценка потенциальных ущербов (по итогам тренировок)*
- Соответствие результатов тренировок – целевым показателям на квартал [

* Важно описать систему зрелости и понимать цикличность развития всех качественных показателей, как и количественных

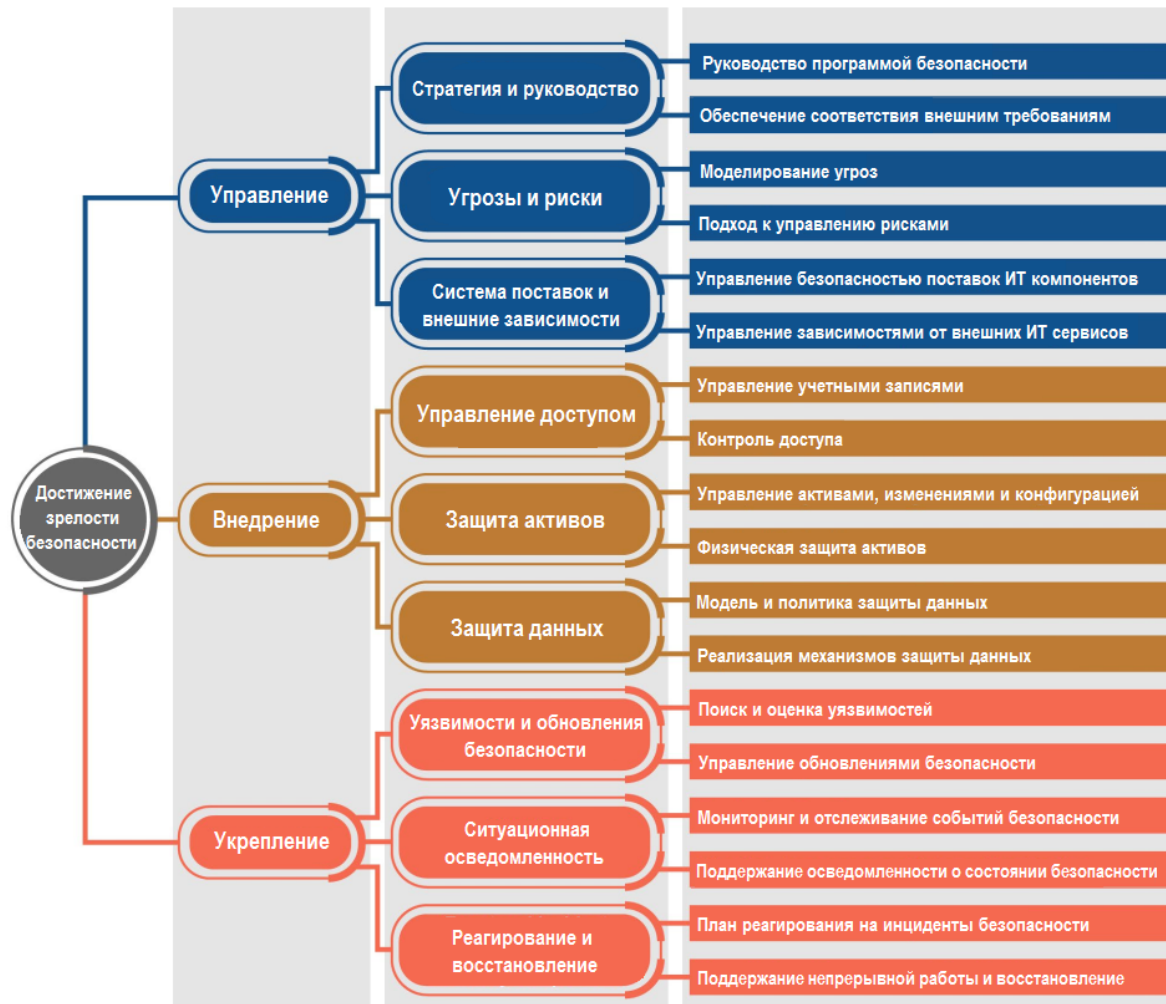
Шаг 5.

Реализовывать описанные процессы и отслеживать успешность реализации



Целевое состояние на примере модели зрелости IoT

[IoT Security Maturity Model: Description and Intended Use White Paper](#)



Открытые системы получения знаний

Открытая база знаний по
Кибербезопасности



EnergyNet

<https://github.com/SecureEnergyNet/Research>

Открытая группа по кибербезопасности

RUSCADASEC

www.discord.gg/nJrmgM9sm.ru

t.me | RuScadaSec

Ассоциация по вопросам
защиты информации



BISA BUSINESS INFORMATION
SECURITY ASSOCIATION

<https://bisa.ru/>