КОД ИБ | ТЮМЕНЬ 2025

Интеграция информационных и операционных технологий с точки зрения обеспечения ИБ

Христолюбова Анна Анатольевна

Отраслевой центр компетенций по ИБ в промышленности Минпромторга России

НПП “Гамма”

ФГУП «НПП «ГАММА»
ЕКАТЕРИНБУРГСКИЙ НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР
27 февраля 2025 г.

КОНТЕКСТ ИБ: IT vs. OT

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

фокус на **конфиденциальности, целостности и доступности данных** (триада CIA)

- Информационные технологии (ИТ) - совокупность методов, процессов и программно-аппаратных средств для обеспечения обработки данных.
- Модель OSI (сервера, коммутаторы, линии связи, информационные системы (ERP, PLM и т.д.)
- Поддержание целевых показателей бизнес-процессов (время выполнения)

ОПЕРАЦИОННЫЕ ТЕХНОЛОГИИ

приоритет — **безопасность и бесперебойность производственных процессов**

- Операционные технологии (ОТ) - аппаратные и программные системы, используемые для управления, мониторинга и автоматизации физических процессов.
- Многоуровневая архитектура (контроллеры, MES , SCADA, PLC, IoT и т.д.), международный стандарт IEC 61499.
- Выпуск продукции (качество, количество, время)

Реальность субъекта КИИ

Методы и средства обеспечения безопасности ОТ и ИТ существенно отличаются (традиционные СЗИ и меры защиты не подходят)

Кто-то один должен нести ответственность на предприятии за обеспечение безопасности объектов КИИ…

Требования НПА не учитывают особенности многоуровневой архитектуры систем, использующих операционные технологии

Возложение задач за пределами компетенции специалистов по ИБ

Увеличение поверхности атаки (сложная архитектура, нераспространенные протоколы передачи данных)

СЛОЖНОСТИ

НЕДООЦЕНКА РЕАЛЬНЫХ УГРОЗ

- Руководители и специалисты по ИБ часто недооценивают уровень угроз, что может привести к отсутствию необходимых мер по защите. Это связано с недостатком информации о реальных рисках и последствиях атак на информационную инфраструктуру

НЕСОВЕРШЕННАЯ СИСТЕМА УПРАВЛЕНИЯ ПРОЦЕССАМИ ИБ НА ПРЕДПРИЯТИИ

- Структура управления на промышленных предприятиях может быть запутанной, что затрудняет принятие решений по вопросам информационной безопасности. Это может привести к задержкам в реагировании на инциденты.

СЛОЖНОСТИ ИНТЕГРАЦИИ ОТ и ИТ

- Совмещение информационных технологий (ИТ) и операционных технологий (ОТ) создает дополнительные вызовы для информационной безопасности. Разные подходы к управлению рисками и безопасности могут привести к конфликтам и уязвимостям.

ОТСУТВИЕ КОМПЛЕКСНОГО ПОДХОДА К ПРОЦЕССАМ ИБ

- Многие предприятия не имеют четко прописанных стратегий ИБ, учитывающих все аспекты ИТ и ОТ, что делает их более уязвимыми для атак злоумышленников и недостижения целей защиты. Необходимость интеграции различных мер защиты в единую систему часто игнорируется.

Результативность vs. Разумность

Результативная ИБ направлена на достижение конкретных результатов, тогда как разумная ИБ больше ориентирована на сбалансированный подход к управлению рисками.

Результативная ИБ

Измеримость: результаты обеспечения ИБ могли быть оценены и подтверждены. Это включает в себя использование метрик, тестов на проникновение (пентестов) и программ bug bounty для проверки защищенности

Фокус на рисках: Определение недопустимых событий и их предотвращение становится основой для построения системы безопасности. Это позволяет сосредоточить ресурсы на наиболее критичных аспектах защиты

Вовлеченность руководства: Высшее руководство активно участвует в формировании стратегии информационной безопасности, что позволяет лучше учитывать реальные потребности бизнеса

Разумная ИБ

Баланс между затратами и безопасностью: стремится найти оптимальное соотношение между затратами на безопасность и уровнем защиты. Это может включать в себя использование стандартных практик и технологий без чрезмерных инвестиций

Гибкость: Подходы к безопасности могут варьироваться в зависимости от конкретных обстоятельств и потребностей бизнеса, что позволяет более адаптивно реагировать на изменения внешней среды.

Учет бизнес-процессов: В отличие от результативной безопасности, разумная безопасность может не всегда иметь четкие измеримые цели. Она больше ориентирована на поддержание стабильности бизнес-процессов при разумном уровне риска

ЛЮБАЯ ПРОБЛЕМА ИМЕЕТ РЕШЕНИЕ©

ПРОБЛЕМА	ПРОБЛЕМА	ПРОБЛЕМА
ОТСУТВИЕ КОМПЛЕКСНОГО ПОДХОДА К ПРОЦЕССАМ ИБ	ИНТЕГРАЦИЯ ОТ и ИТ	НЕСОВЕРШЕННАЯ СИСТЕМА УПРАВЛЕНИЯ ПРОЦЕССАМИ ИБ НА ПРЕДПРИЯТИИ
РЕШЕНИЕ	**РЕШЕНИЕ**	**РЕШЕНИЕ**
Построение архитектурной модели	Построение процессной и функциональной модели на базе товарной матрицы, оценка влияния ОТ и ИТ на процессы	Количественная и качественная оценка распределения ответственности и организационно-штатной структуры вертикали управления ИБ
МЕТОД	**МЕТОД**	**МЕТОД**
NIST Enterprise Architecture (NIST EA)	BIA (Business Impact Analysis), Эталонная модель основного производства по ГОСТ Р 34.1501.1-92. Торгово-технологический процесс оказания услуг оптовой торговли по ГОСТ Р 51304-2022. Жизненный цикл изделия ВТ по ГОСТ РВ 0015-002.	Типология организационных структур предприятий по Генри Минцбергу

Целевые модели (уровни) архитектуры

МОДЕЛЬ ОЦЕНКИ РЕЗУЛЬТАТИВНОСТИ (Performance Reference Model, PRM)
Определяет измеримые показатели результативности, которые помогают оценивать уровень и качество реализации системы управления ИБ.
ВЛАДЕЛЕЦ: заместитель генерального директора, уполномоченный в вопросах информационной безопасности

ФУНКЦИОНАЛЬНАЯ МОДЕЛЬ ДЕЯТЕЛЬНОСТИ (Business Reference Model, BRM)
Описывает пути развития и поддержания внутренних процессов и процедур в области обеспечения информационной безопасности в Обществе.
ВЛАДЕЛЕЦ: Руководитель структурного подразделения по ИБ

МОДЕЛЬ СЕРВИСОВ (Service Component Reference Model, SRM)
Описывает выполнение основных операций и задач, реализованных в качестве сервисов информационной безопасности (как внешних, так и внутренних).
ВЛАДЕЛЕЦ: Специалист по информационной безопасности

МОДЕЛЬ ДАННЫХ (Data Reference Model, DRM)
Описывает структуру и содержание данных, используемых в Обществе, помогает стандартизировать формат и процедуры управление данными, обеспечивая их свойства безопасности.
ВЛАДЕЛЕЦ: Специалист по информационной безопасности, руководители структурных подразделений

ТЕХНИЧЕСКАЯ МОДЕЛЬ (Technical Reference Model ,TRM)
Описывает технические стандарты и технологии, которые используются для обеспечения информационной безопасности.

ВЛАДЕЛЕЦ: начальник отдела ИТ, Главный системный администратор вычислительной сети Общества, начальник отдела АСУ ТП

Влияние компьютерных инцидентов на производство основной продукции (услуги)

BIA (Business Impact Analysis)

ВЫСОКО КРИТИЧНЫЙ ПРОЦЕСС	СРЕДНЕ КРИТИЧНЫЙ ПРОЦЕСС	НИЗКО КРИТИЧНЫЙ (НЕКРИТИЧНЫЙ) ПРОЦЕСС
RTO: 1–2 часа (простой приводит к значительным финансовым потерям, возникает риск ответственности для руководителей за срыв сроков).	RTO: 24 часа (задержки в получении результата могут привести к штрафам, но не к остановке производства основной продукции).	RTO: 72 часа (временные задержки не критичны для деятельности Общества)
Интерпретация: Процесс напрямую влияет на выполнение условий контракта по срокам и на прибыль Общества.	Интерпретация: Процесс существенен для результата, но его остановка не приводит к немедленным катастрофическим последствиям для выполнения условий контракта по срокам и на прибыль Общества.	Интерпретация: Процесс не влияет напрямую на условий контракта по срокам и на прибыль Общества.

Допустимое время простоя (Recovery Time Objective, RTO)

Время восстановления функционирования процесса (Actual Recovery Time, ART)

Пример BIA (Business Impact Analysis) для процесса «*Входной контроль, производственный контроль и испытания*»

ИСХОДНЫЕ ДАННЫЕ:

Процессная и функциональная модель, включающая в себя все ресурсы (персонал, энергетика, вода, сжатый воздух, СКУД, станки, доступ в Интернет и т.д.), с описанием влияния ОТ и ИТ на достижение целевых показателей процесса

«Входной контроль, производственный контроль и испытания»		
Максимально допустимое время простоя, в течение которого ресурс должен быть восстановлен (Recovery Time Objective)	RTO = 2 дня (48 часов, 2 880 минут) (среднекритичный процесс)	Простой более 2 дней приводит к значительным финансовым потерям и срыву сроков выполнения условий государственного контракта.
Прогнозируемое время восстановления функционирования (целевых показателей процесса) (Actual Recovery Time)	ART=4 час 20 минут (270 минут).	Шаги восстановления: 1. Обнаружение сбоя: 10 минут. 2. Диагностика проблемы: 20 минут. 3. Восстановление данных из резервной копии: 2 часа. 4. Восстановление и проверка работоспособности оборудования: 1 час 30 минут. 5. Запуск испытаний, контроля: 20 минут.
Анализ	ART (270 минут) < RTO (48 часов, 2 880 минут) — процесс восстановлен в рамках допустимого времени.	

Оценка эффективности вертикали управления ИБ

Содержание метрики	Домены метрики	Результат оценки метрик
Параметры индивидуальной деятельности	Межличностные роли	
	Информационные роли	
	Решающие роли	
Структурные параметры	Иерархия	
	Централизация	
	Формализация	
	Специализация	
	Стандартизация	
	Координация	
	Интеграция	
Параметры системы принятия решений	Цели и приоритеты	
	Процесс принятия решений	
	Роли и ответственность	
	Коммуникация	
	Время принятия решений	
	Качество решений	
	Обратная связь и обучение	
	ИТОГО	47 % (8) / 41 % (7) / 12 % (2) / 0 % (0)

Не соответствует целям результативности системы обеспечения информационной безопасности в Обществе	Требует корректировки мероприятий по обеспечению информационной безопасности в Обществе	В целом соответствует целям результативности системы обеспечения информационной безопасности в Обществе	Соответствует целям результативности системы обеспечения информационной безопасности в Обществе

Полномочия и обязанности сторон

Отраслевой центр компетенций по ИБ в промышленности Минпромторга России

https: //ock.gammaural.ru

t.me/ockgammaural