Требования КИИ, что на первом месте: люди или технологии?

КОНСТАНТИН САМАТОВ

Руководитель комитета по безопасности КИИ,
член Правления АРСИБ.

Что на первом месте: люди или технологии?

Приказ ФСТЭК России от 21.12.2017 № 235
"Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования"

Люди

Требования к работникам структурного подразделения по обеспечению безопасности объектов КИИ

С 01.01.2021 (Приказ ФСТЭК России от 27 марта 2019 г. № 64)

Руководитель подразделения:

- Высшее образование по ИБ и стаж свыше 3 лет
- Иное высшее образование и профессиональная подготовка по ИБ (не менее 360 часов) и стаж свыше 3 лет

Штатный специалист:

- Высшее образование по ИБ
- Иное высшее образование + курс повышения квалификации по ИБ (не менее 72 часов)

Не реже одного раза в пять лет обучение по программе повышения квалификации по направлению подготовки «Информационная безопасность»

CISO BISO ISO

Где взять?

- СУЗ/ВУЗ
- Рынок
- Комьюнити

Как удержать?

Процессы

Планирование и разработка мероприятий (Plan)

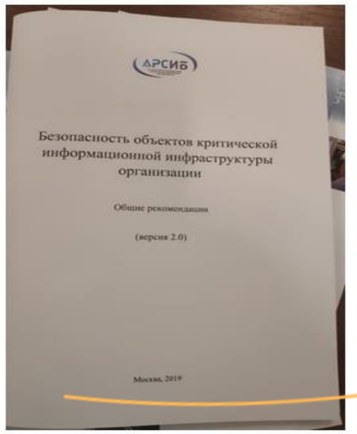
Реализация (внедрение) мероприятий (Do)

Объекты КИИ (ИС, ИТКС, АСУ)

Совершенствование безопасности (Act)

Контроль состояния безопасности (Control)

Эдвардс Деминг (1900 – 1993)



НКЦКИ
НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Технологии

Уровень управления	Инструмент автоматизации	Какие процессы автоматизирует
Стратегический	Security GRC (Governance, Risk, Compliance)	Процессы планирования, внедрения, мониторинга, контроля и совершенствования
Функциональный	SOAR (Security Orchestration, Automation and Response)	Процесс управления инцидентами и уязвимостями, включая автоматический ответ на инциденты
	IdM (Identity Management)	Процесс управления доступом
	IDS (Intrusion Detection System)/ IPS (Intrusion Prevention System)	Процесс обнаружения (предотвращения) вторжений
	DLP (Data Leak Prevention)/ UAM (User Activity Monitoring)/ UEBA (User and Entity Behavior Analytics)	Процесс предотвращения утечек и (или) контроля персонала
	EDR (Endpoint Detection and Response)	Процесс защиты от вредоносного программного обеспечения
	MDM (Mobile Device Management)	Процесс управления мобильными устройствами
Операционный	Данный уровень представлен клиентской частью (агентами) обозначенных на предыдущем уровне инструментов, которая осуществляет сбор информации и управление подсистемами безопасности конкретных информационных активов	

Спасибо за внимание

Ваши вопросы

КОНСТАНТИН САМАТОВ

Руководитель комитета по безопасности КИИ,
член Правления АРСИБ.