АСТАНИНСКИЙ ЭКОНОМИЧЕСКИЙ ФОРУМ 2019

Секция 2. Процессы, технологии, кадры. Фундамент цифровой безопасности

Стефанов Руслан

16.05.2019

Рекомендуемая производителем АСУ ТП практика киберзащиты в промышленности

Honeywell

HONEYWELL В КАЗАХСТАНЕ

1998 Открытие офиса в Алматы

3 Офиса: Алматы, Атырау, Нур-Султан

>70 Человек

Учебный центр в Атырау

Ключевые отрасли:

- Нефтегазовая, горнорудная, нефтехимия
- Здания, сооружения, инфраструктура
- Ритейл, логистика

Бизнесы/департаменты:

- Промышленная автоматизация (Process Solutions)
- Системы и сервис зданий (Building Solutions)
- Промышленная безопасность (Industrial Safety)
- Нефте- и газопереработка, нефтехимия (Honeywell UOP)

Honeywell

Программа развития талантов

- 1 марта 2019 г. подписано соглашение о создании Центра Автоматизации в КБТУ
- Для обучения студентов по специальности “автоматизация и управление” и повышения квалификации операторов, инженеров-технологов нефтегазовых и горно-добывающих компаний.
- Новейшее ПО и оборудование Honeywell.
- Цели - снижение ошибок операторов, улучшение производственной эффективности и безопасности промышленных предприятий.

KAZAKH BRITISH TECHNICAL UNIVERSITY

Honeywell

Новости Honeywell Industrial Cybersecurity

- Первые в мире контроллеры ControlEdge™, получившие сертификаты ISASecure® Embedded Device Security Assurance (EDSA) Level 2
  - http://www.isasecure.org/en-US/End-Users/ISASecure-Certified-Devices

- Обновления портфеля решений по киберзащите
  - Квалифицировано решение Carbon Black (контроль «белых списков и сменных носителей)
  - Новая версия Secure Media Exchange
  - Новая версия ICS Shield
  - Новая версия Risk Manager R170
  - Расширение услуг Cyber Vantage Managed Security Services (MSS)

CARBON BLACK
ARM YOUR ENDPOINTS

Honeywell

Honeywell Industrial Cyber Security

Эксперты по безопасности

- Глобальная команда сертифицированных специалистов по промышленной безопасности
- 100% разработка и поддержка кибер-безопасности
- Эксперты в области управления технологическими процессами кибер-безопасности

Проверенный Опыт работы

- 10+ опыта работы
- 1,000+ успешных проектов
- 300+ прямая поддержка предприятий
- Фирменные Методологии и инструменты

Инвестиции и инновации

- Инвестиции в исследования
- Стратегическое патрнерство с производителями в информационной безопасности
- Система управления риском

Переработка

нефтегаз

Химия

Энергетика

Добыча

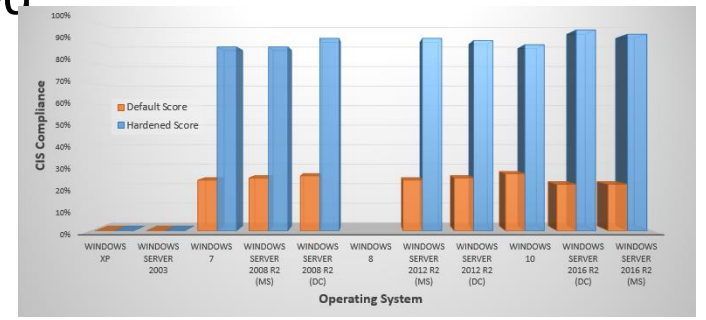
Деревообработка

Honeywell

Портфель решений

Услуги на базе рекомендаций CIS

- CIS (Center for Internet Security, Inc.) является некоммерческой организацией, которая использует возможности глобального ИТ-сообщества для защиты частных и общественных организаций от киберугроз.
- Межгосударственный центр обмена информацией и анализа
- CIS-CAT Pro Assessor - A Deeper Dive
- May 21, 2019 at 11:30 am EDT
- CIS Benchmarks™ – Understand, implement, plan and get involved
- May 23, 2019 at 1:30 pm EDT



- Укрепление защиты (PCN Hardening) включает:
  - Доменные групповые политики
  - Отключение не используемых сервисов
  - Определение прав пользователей
  - CIS Benchmarks (измерение уровня защищенности по метрикам)

CIS® Center for Internet Security®

Honeywell

Услуга Cyber Security HAZOP

- Исследование csHAZOP может быть выполнено на уровнях Level 1 и Level 2
- Эксперты Honeywell OT security HAZOP следуют стандарту IEC 61882:2016 в части методологии и применения специальных инструментов (HAZOP worksheet, checklists, Amenaza Attack Tree modelling tool) при проведении csHAZOP.

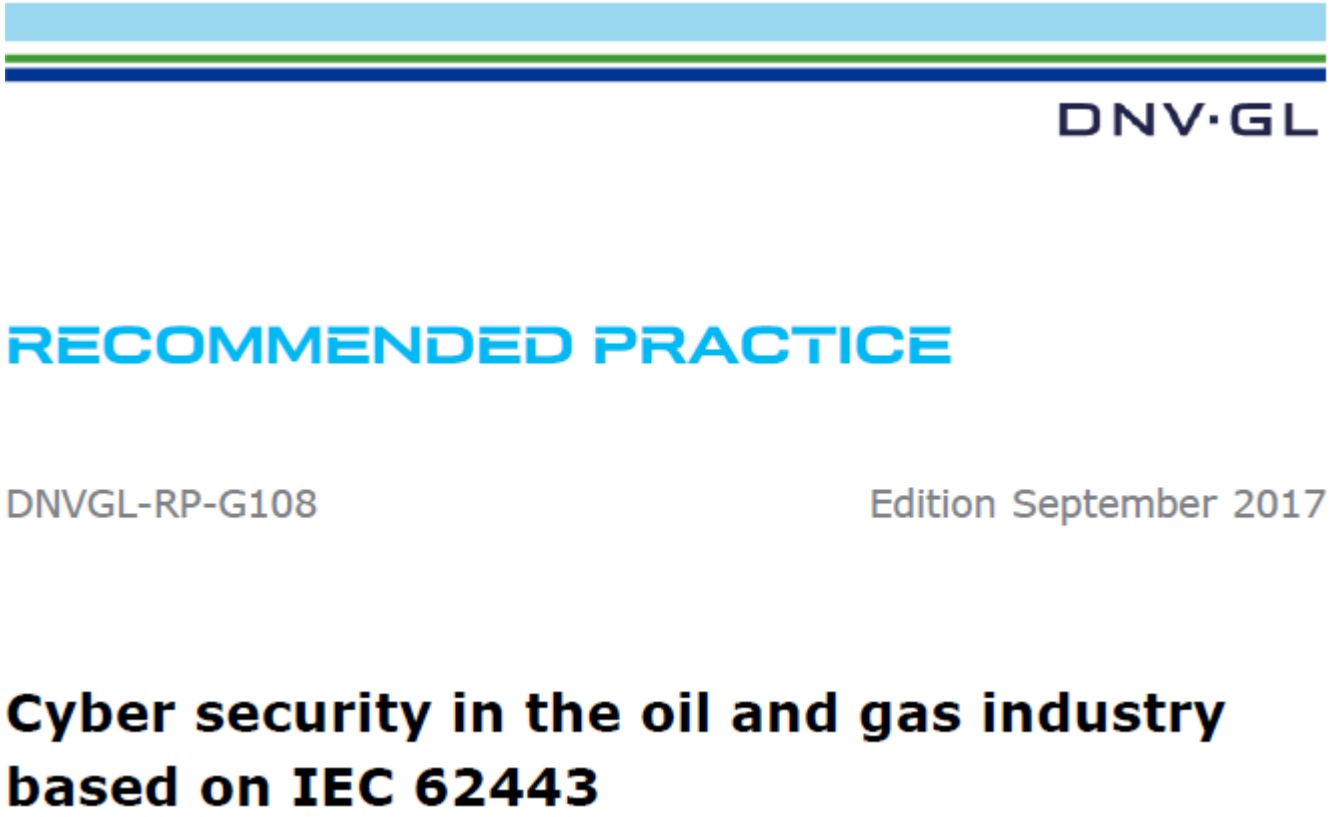
Increasing consequences →	Severity	Consequence Categories			Increasing probability				
		Safety	Environment	Cost (million Euro)	1	2	3	4	5
					Failure is not expected $< 10^{-5}$	Never heard of in the industry $10^{-5} - 10^{-4}$	An accident has occurred in the industry $10^{-4} - 10^{-3}$	Has been experienced by most operators $10^{-3} - 10^{-2}$	Occurs several times per year $10^{-2} - 10^{-1}$
	E	Multiple fatalities	Massive effect Large damage area, > 100 BBL	> 10	M	H	VH	VH	VH
	D	Single fatality or permanent disability	Major effect Significant spill response, < 100 BBL	1 - 10	L	M	H	VH	VH
	C	Major injury, long term absence	Localized effect Spill response < 50 BBL	0.1 - 1	VL	L	M	H	VH
	B	Slightly injury, a few lost work days	Minor effect Non-compliance, < 5 BBL	0.01- 0.1	VL	VL	L	M	H
	A	No or superficial injuries	Slightly effect on the environment, < 1BBL	< 0.01	VL	VL	VL	L	M

Honeywell

Joint Industry Project (Норвегия)

- Section 1 General
- Section 2 Definitions and abbreviations
- Section 3 Concept phase
- Section 4 FEED phase
- Section 5 Project phase
- Section 6 Operations phase
- Section 7 References
- Appendix A Example of a cyber security requirement specification
- Appendix B Detailed risk assessment workflow

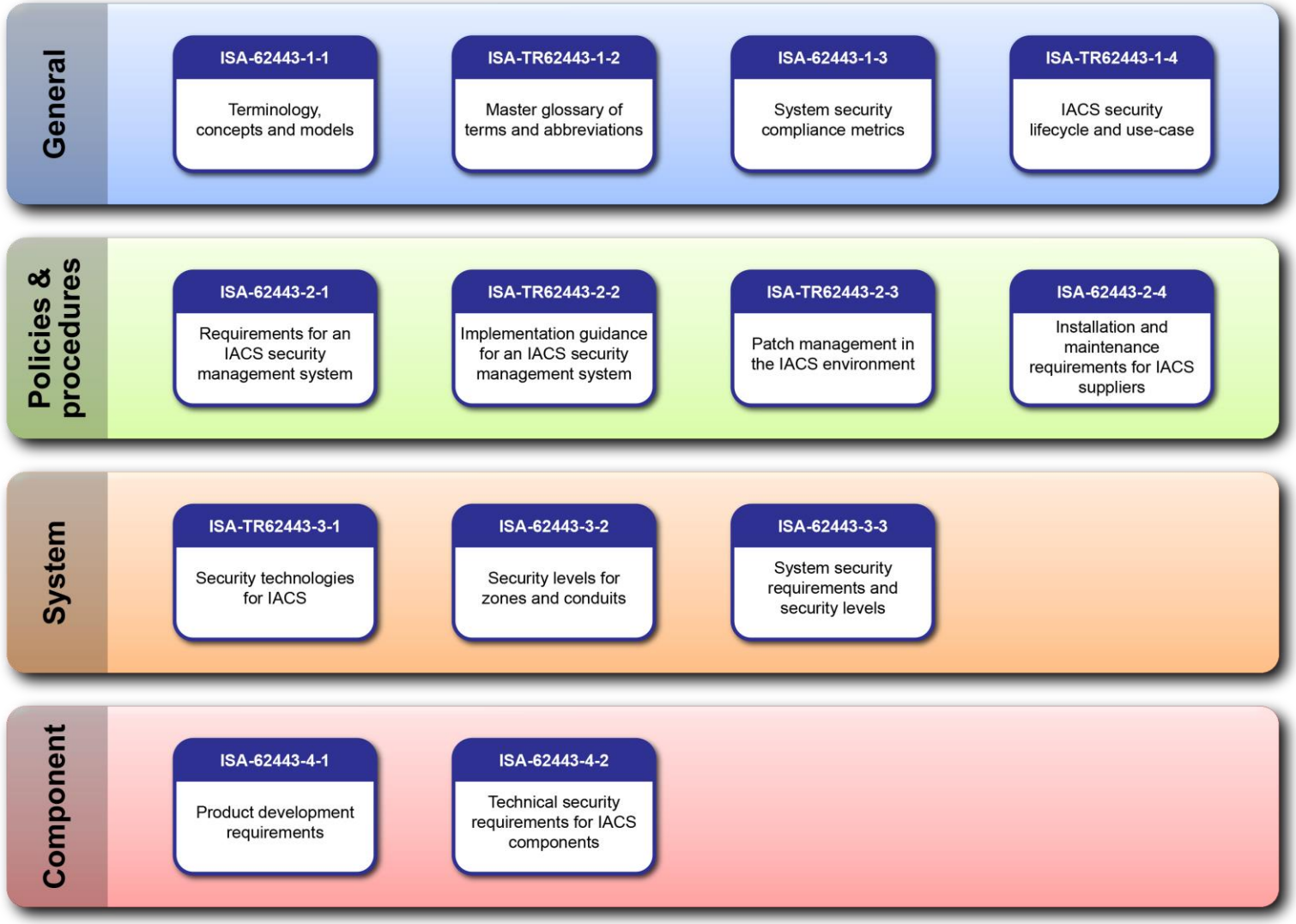
https://www.dnvgl.com/oilgas/download/dnvgl-rp-g108-cyber-security-in-the-oil-and-gas-industry-based-on-IEC-62443.html



Honeywell

IEC 62443 (Международный стандарт)

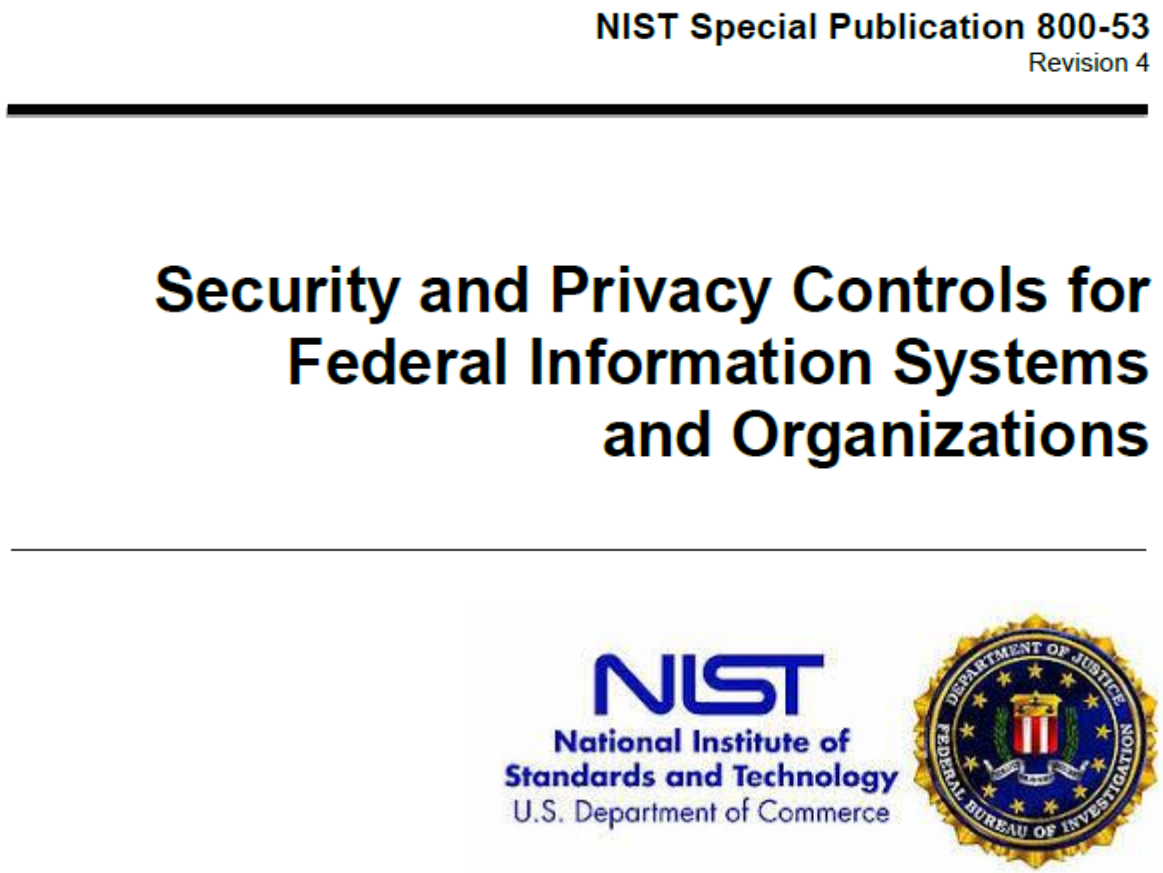
ГОСТ Р МЭК 62443… «Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы»



Honeywell

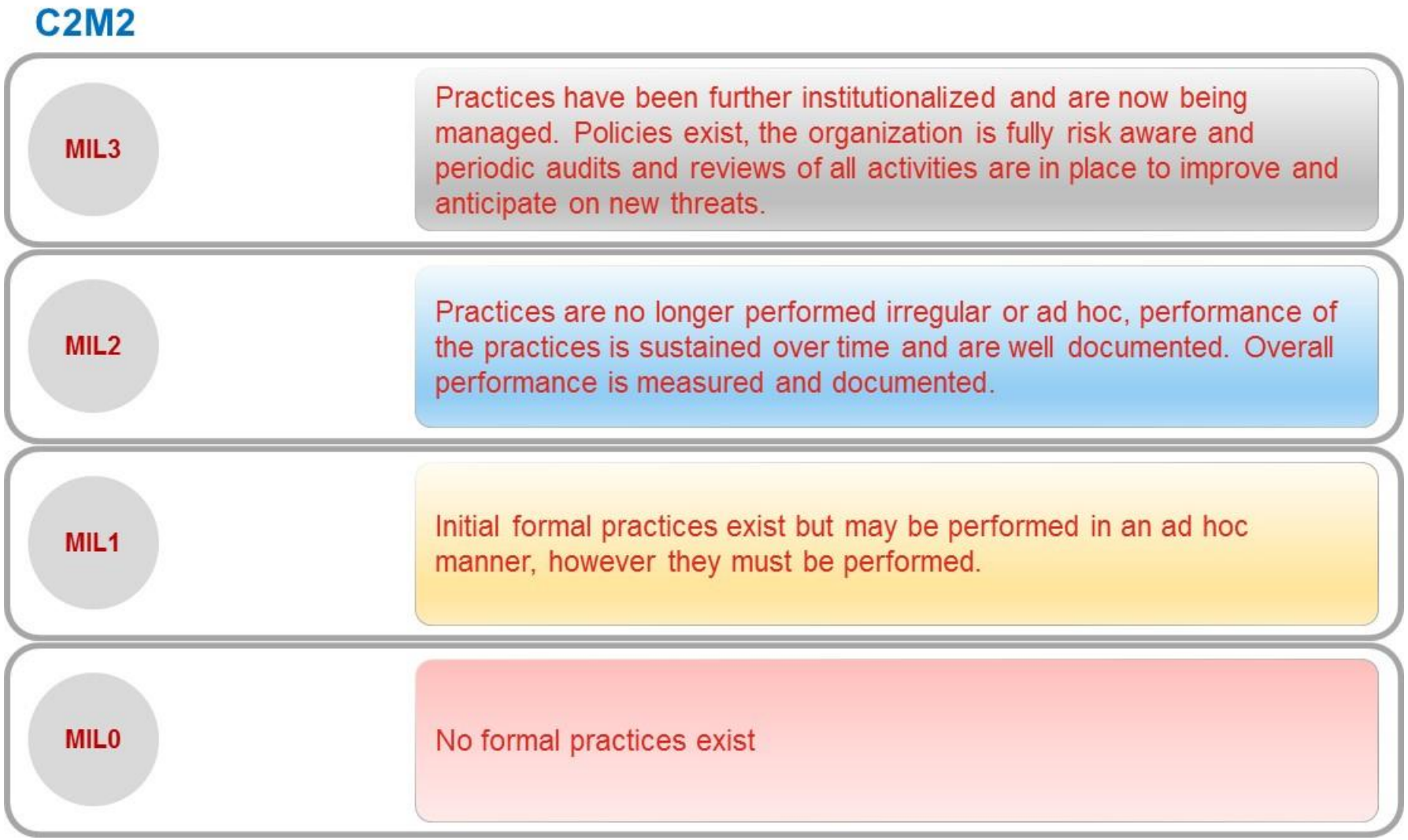
NIST SP 800-53 (US)

- The fundamentals
  - Multitiered risk management
  - Security control structure
  - Security control baselines
- The process
  - Selecting security control baselines
  - Tailoring baseline security controls



Honeywell

Cybersecurity Capability Maturity Model (US)



Honeywell

ФЗ №187 О безопасности КИИ (Россия)

- В январе 2018 года в РФ вступил в силу Федеральный закон от 26 июля 2017 г. N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

- Правила и критерии категорирования объектов КИИ (Постановление Правительства РФ от 8 февраля 2018 г. №127)
- Требования к созданию систем безопасности значимых объектов КИИ (Приказ ФСТЭК от 21.12.2017 №235)
- Требования по обеспечению безопасности значимых объектов КИИ (Приказ ФСТЭК от 25.12.2017 г. № 239)

Honeywell

Networks and Information Systems Directive (EU)

- Is aimed specifically at critical infrastructure, including:
  - Operators of Essential Services (OESs) - e.g. oil, gas, energy, transportation, banking, water, food and telecommunications
  - Digital Service Providers (DSPs)

Honeywell

Актуальные проблемы цифровой безопасности

"До 2020, 99% эксплуатируемых уязвимостей будут составлять уже не менее одного года известные профессионалам уязвимости" *

- Рекомендуемые действия: Упор на блокирование атак, использующих "известные уязвимости"

"До 2020, треть успешных атак на предприятиях будут приходиться на теневые (не учтенные) ресурсы IT" *

- Рекомендуемые действия: организации должны инвестировать в свою способность обнаруживать и следить за использованием теневых ресурсов IT в подразделениях

* Gartner Essentials: Top Security Predictions/SPAs 2016" John A. Wheeler, Gartner Security & Risk Management Summit, 13–16 June 2016 | National Harbor, MD

Honeywell

Рекомендации производителя

- Участие производителя на всех этапах создания системы безопасности (СБ)
  - Формирование требований СБ (моделирование угроз, анализ рисков, csHAZOP)
  - Проектирование (применение лучших практик и решений производителя)
  - Внедрение (оценка соответствия СБ производителем)
  - Эксплуатация поддерживаемых систем
    - Миграции решают проблему не поддерживаемых систем
    - Сервис от производителя (обновления, аутсорсинг) поддерживает системы в актуальном состоянии
- Практическая подготовка казахских специалистов в области кибербезопасности (например в рамках сервисной модели «виртуальный инженер/консультант по кибербезопасности»)

Honeywell

Спасибо за внимание

www.becybersecure.com

Honeywell