ЦИФРОВЫЕ ДВОЙНИКИ И ПОДХОДЫ К ОБЕСПЕЧЕНИЮ ИХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Директор Научно-образовательного центра
новых информационно-аналитических технологий
факультета комплексной безопасности ТЭК
РГУ нефти и газа (НИУ) им. И.М.Губкина
к.т.н. Д.И.Правиков

СТАНДАРТЫ ЦИФРОВЫХ ДВОЙНИКОВ

- ПНСТ 428-2020 Умное производство. Двойники цифровые производства. Элементы визуализации цифровых двойников производства
- ПНСТ 429-2020 Умное производство. Двойники цифровые производства. Часть 1. Общие положения
- ПНСТ 430-2020 Умное производство. Двойники цифровые производства. Часть 2. Типовая архитектура
- ПНСТ 431-2020 Умное производство. Двойники цифровые производства. Часть 3. Цифровое представление физических производственных элементов
- ПНСТ 432-2020 Умное производство. Двойники цифровые производства. Часть 4. Обмен информацией

ПРИМЕНЕНИЕ ЦИФРОВЫХ ДВОЙНИКОВ

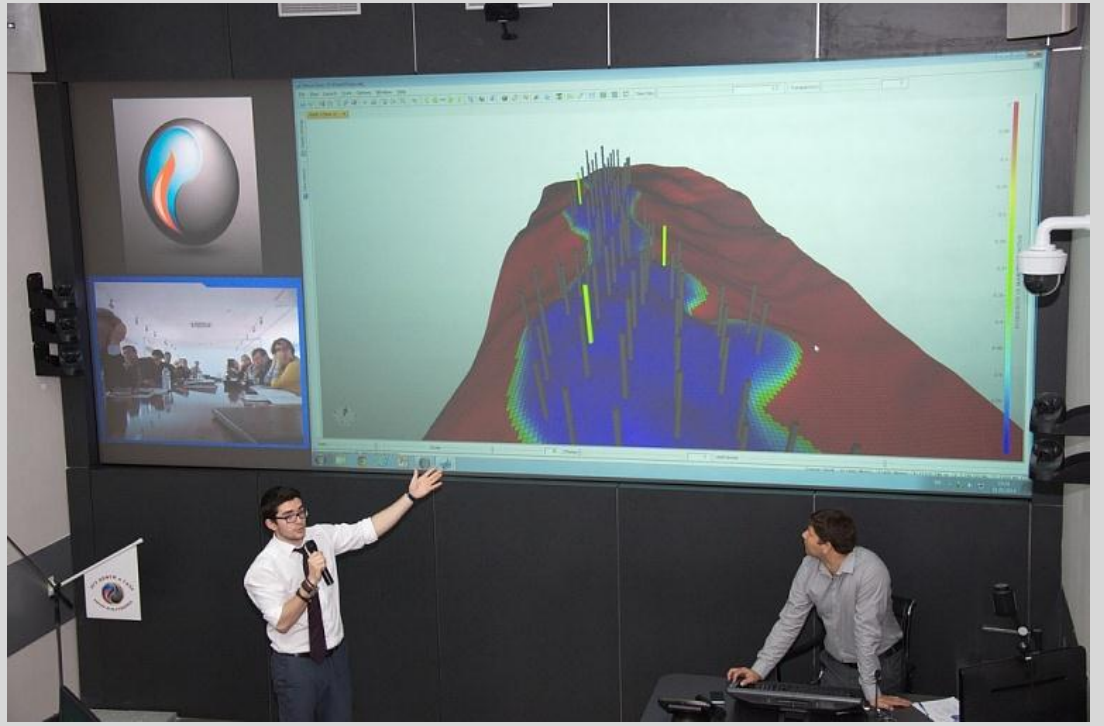
Энергетическая стратегия до 2035 г.

Перечень технологического оборудования, востребованного организациями топливно-энергетического комплекса Российской Федерации, создание или локализация производства которого необходимы на территории Российской Федерации до 2035 года (п. 30)

Практика в ТЭК

- «Цифровое месторождение»
- «Цифровой НПЗ»

РАЗРАБОТКА «ЦИФРОВЫХ» МЕСТОРОЖДЕНИЙ



«ЦИФРОВОЙ НПЗ»

ЦИФРОВОЙ ДВОЙНИК

Системы 3d-моделирования используются для создания цифровых двойников оборудования на НПЗ «Газпром Нефти»

«Сибирская нефть»
№3/140 Апрель 2017

ПРИМЕРЫ РЕАЛИЗАЦИИ УГРОЗ ЦИФРОВЫМ МОДЕЛЯМ ОБЪЕКТА

Авария ракеты-носителя «Союз-2.1б» со спутником «Метеор-М».
Космодром «Восточный».
28 ноября 2017 года

Крушение пассажирского самолета Ан-148 авиакомпании «Саратовские авиалинии».
Раменский район Московской области.
11 февраля 2018 года

НОВЫЙ ВИД УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Основная угроза информационной безопасности - угроза несоответствия модели («цифрового двойника») реальному объекту. Следствие – снижение качества управления.

Проблема обеспечения информационной безопасности «цифрового двойника» - для большинства объектов модель («цифровой двойник») не может быть статической.

ФОРМАЛИЗАЦИЯ ПОНЯТИЯ «ЦИФРОВОГО ДВОЙНИКА»

«Цифровой двойник» опишем как систему асимптотической оценки для линейной стационарной управляемой системы $\dot{X} = AX + BU$ в условиях неполной информации

$$\dot{\hat{X}} = A\hat{X} + BU + \sum_{i=1}^{n} L_i \left(y_i - R^* \hat{X}(t - i\tau)\right)$$

если вектора-столбцы L_i выбраны так, что выполняется условие

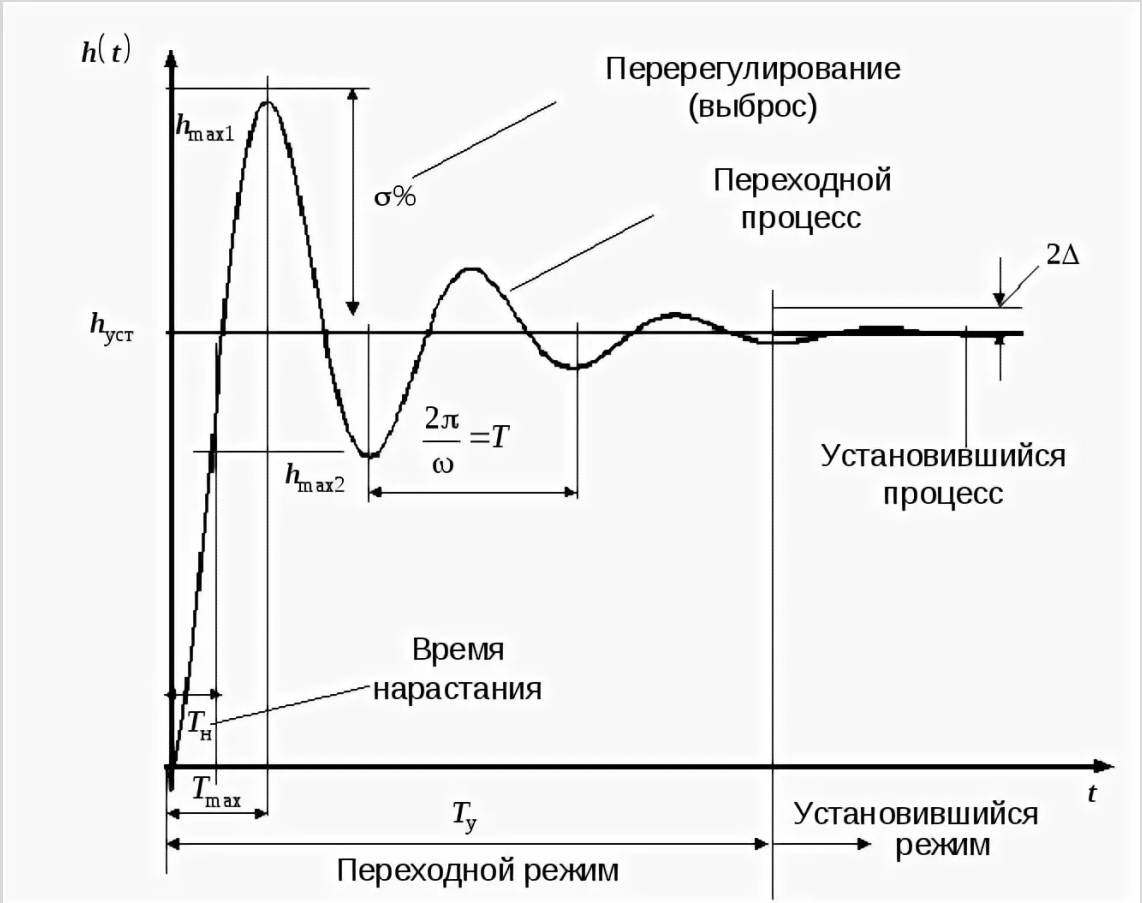
$$\hat{X}(t) - X(t) \to 0 \text{ при } t \to \infty$$

где *X* – вектор состояния, *U* – вектор управления, *R* – постоянная вектор-строчка, *τ* – постоянная запаздывания.

ОЦЕНКА ЗАЩИЩЕННОСТИ ЧЕРЕЗ КАЧЕСТВО УПРАВЛЕНИЯ

Защищенность «цифрового двойника» можно определить через качество переходного процесса при подаче единичного воздействия.

Вместе с тем, общепризнанные подходы к защите «цифровых двойников» отсутствуют.



АКТУАЛЬНАЯ УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Реализация «цифровых двойников» – передача данных, собираемых с киберфизических устройств в «облако», где проводится их обработка.

Проблема: существующие решения в основном импортные, поэтому данные передаются в «облака», находящиеся за рубежом.
Не обеспечивается технологическая независимость.

Требования регулятора (новая редакция приказа ФСТЭК России № 239) предусматривают обработку данных на территории Российской Федерации для значимых объектов КИИ 1 и 2 категории.

РАЗРАБОТКА НАУЧНЫХ ОСНОВ БЕЗОПАСНОСТИ ЦИФРОВЫХ ДВОЙНИКОВ

- Российский государственный университет нефти и газа (НИУ) имени И.М. Губкина
- Санкт-Петербургский государственный политехнический университет имени Петра Великого

ВЫВОДЫ

1. Цифровые двойники являются технологией, которая уже начала применяться в различных сферах промышленности и энергетики.
2. Применение цифровых двойников порождает новые виды угроз информационной безопасности, которые ранее не рассматривались.
3. Необходима разработка требований, методов и средств обеспечения информационной безопасности цифровых двойников.