АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ
«Защита информации в киберфизических системах»

по основной профессиональной образовательной программе по направлению подготовки 10.03.01 «Информационная безопасность» (уровень бакалавриата)

Направленность (профиль): Организация и технологии защиты информации (в сфере техники и технологий, связанных с обеспечением защищенности объектов информатизации)
Общий объем дисциплины – 5 з.е. (180 часов)
Форма промежуточной аттестации – Экзамен.
В результате освоения дисциплины у обучающихся должны быть сформированы компетенции с соответствующими индикаторами их достижения:
- ПК-4.1: Демонстрирует знание методов исследования защищенности объектов и средств защиты;
- ПК-4.2: Предлагает методы исследования объектов информатизации с учетом их особенностей;

Содержание дисциплины:
Дисциплина «Защита информации в киберфизических системах» включает в себя следующие разделы:
Форма обучения очная. Семестр 7.
1. Введение. Общее представление о киберфизических системах. АСУ ТП. Интернет вещей - IoT и IIoT системы. SCADA – системы.
2. Примеры киберфизических систем. Киберфизические системы в автомобилестроении. Киберфизические системы в строительстве, сельском хозяйстве, машиностроении, ЖКХ. СКУД как киберфизическая система. Коллективы автономных роботов как пример киберфизических систем в наземном, воздушном и водном транспорте.
3. Характеристики мониторинга безопасности киберфизических систем. Таксономия аварий и катастроф. Методы исследования защищенности киберфизических систем с учетом их особенностей, способы описания и анализа их свойств безопасности. Проблемы, связанные с обеспечением безопасности сложных энергонасыщенных систем. Показатели и критерии безопасности систем. Киберфизическая система как объект управления информационной безопасностью и ее модель угроз с точки зрения теории управления. Характеристики мониторинга безопасности.
4. Интерфейсы киберфизических систем. Field – интерфейсы. Проводные интерфейсы RS – 232, RS – 422, RS – 485, Microlan. Беспроводные интерфейсы Wi-Fi, ZigBee, GSM, WiMax, NFC.
5. Информационно-измерительные преобразователи киберфизических систем. Классификация измерительных преобразователей. Принцип работы основных видов измерительных преобразователей. Исполнительные устройства.
6. Стандарты, платформы и технологии IoT. Архитектура IoT и IIoT систем. LoRaWan, LTE-M, Sigfox, NB-IoT, BLE, Z-Wave - краткая характеристика и особенностей распространения радиосигнала.
7. SCADA-системы. Архитектура SCADA-систем. Программируемые логические контроллеры (ПЛК). Промышленные компьютеры. Краткая характеристика современных SCADA систем.
8. Основы методологии обоснования требований к безопасности технических систем и обеспечения этих требований. Закономерности развития технических систем. Фундаментальная система факторов, определяющих качество и безопасность системы. Системотехнический анализ развития системы. Модель функционирования технических систем. Вероятностные модели исследования состояний технических систем. Методы обеспечения безопасности киберфизических систем. Управление и регулирование безопасностью и рисками.
9. Методы выявления аномального поведения в работе киберфизических систем. Методы предсказания на основе анализа многомерных временных рядов. Использование механизма NEAT-гиперкуба для обнаружения кибератак на системы IoT. Обнаружение аномалий в киберфизических си-стемах с использованием графовых нейронных сетей. Выявление аномальных ситуаций в сетевых сегментах Интернета вещей на основе ансамбля классификаторов. Применение

технологии Honeypot с адаптивным поведением для отслеживания и анализа атак на сети Интернета вещей. Обеспечение устойчивости киберфизических систем (КФС) на основе теории графов. Выявление аномального функционирования устройств индустрии 4.0 на основе поведенческих паттернов.

Разработал:
заведующий кафедрой
кафедры ИВТиИБ А.Г. Якунин

Проверил:
Декан ФИТ А.С. Авдеев