

Министерство науки и высшего образования Российской Федерации
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Санкт-Петербургский государственный университет промышленных технологий и дизайна»
(СПбГУПТД)

УТВЕРЖДАЮ
Директор ВШТЭ



Рабочая программа дисциплины

Б1.В.09 Промышленный IIoT и кибербезопасность сетевого уровня

Учебный план: _____ ФГОС3++m150404ПИСС-1_26-12.plx

Кафедра: **32** Автоматизации технологических процессов и производств

Направление подготовки: _____
(специальность) 15.04.04 Автоматизация технологических процессов и производств

Профиль подготовки: _____
(специализация) Прикладные информационные системы в сфере автоматизированных систем управления технологическими процессами

Уровень образования: _____ магистратура

Форма обучения: _____ очная

План учебного процесса

Семестр (курс для ЗАО)		Контактная работа обучающихся		Сам. работа	Контроль, час.	Трудоёмкость, ЗЕТ	Форма промежуточной аттестации
		Лекции	Практ. занятия				
3	УП	17	34	56,75	0,25	3	Зачет
	РПД	17	34	56,75	0,25	3	
Итого	УП	17	34	56,75	0,25	3	
	РПД	17	34	56,75	0,25	3	

Рабочая программа дисциплины составлена в соответствии с федеральным государственным образовательным стандартом высшего образования по направлению подготовки 15.04.04 Автоматизация технологических процессов и производств, утверждённым приказом Минобрнауки России от 25.11.2020 г. № 1452

Составитель (и):

Доктор технических наук, профессор

Вагизов Марсель
Равильевич

От кафедры составителя:

Заведующий кафедрой автоматизации
технологических процессов и производств

Ковалев Д.А.

От выпускающей кафедры:

Заведующий кафедрой

Ковалев Д.А.

Методический отдел:

Фахретдинова А. Р.

1 ВВЕДЕНИЕ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

1.1 Цель дисциплины: Формирование у студентов системных знаний и практических навыков в области проектирования, внедрения и обеспечения кибербезопасности промышленных IoT-систем на сетевом уровне.

1.2 Задачи дисциплины:

- Изучить архитектуру и принципы работы промышленных IoT-систем, а также особенности их интеграции с корпоративными и технологическими сетями.
- Рассмотреть основные угрозы и уязвимости, характерные для сетевого уровня промышленных IoT-решений.
- Освоить методы и инструменты анализа защищённости сетевой инфраструктуры IIoT.
- Научиться применять современные подходы и стандарты кибербезопасности для защиты промышленных сетей.
- Развить навыки проектирования и внедрения механизмов обнаружения, предотвращения и реагирования на инциденты в IIoT-системах.

1.3 Требования к предварительной подготовке обучающегося:

Предварительная подготовка предполагает создание основы для формирования компетенций, указанных в п. 2, при изучении дисциплин:

Навыки основ сетевого администрирования и информационной безопасности.

2 КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ПК-3: Способен обосновывать необходимость защиты информации в автоматизированной системе
Знать: стандарты IEC 62443, требования ФСТЭК, актуальные угрозы для IIoT
Уметь: выявлять каналы утечки и несанкционированного доступа
Владеть: методиками анализа рисков информационной безопасности
ПК-2: Способен контролировать разработку проекта автоматизированной системы управления технологическими процессами
Знать: методы контроля защищённости сетевых подключений
Уметь: проверять настройки безопасности IIoT-устройств
Владеть: навыками аудита сетевой безопасности
ПК-7: Способен выбирать технологии и основные компоненты обеспечивающей части создаваемых ИАС
Знать: технологии IIoT (MQTT, LoRaWAN, NB-IoT), шлюзы, Edge-вычисления
Уметь: выбирать способ подключения полевых устройств к ИАС
Владеть: навыками проектирования защищенных каналов передачи данных

3 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Наименование и содержание разделов, тем и учебных занятий	Семестр (курс для ЗАО)	Контактная работа		СР (часы)	Форма текущего контроля
		Лек. (часы)	Пр. (часы)		
Раздел 1. Архитектура и особенности промышленных *IoT*-систем	3				
Тема 1. Архитектура и особенности промышленных IoT-систем		2	4	7	
Раздел 2. Угрозы и уязвимости сетевого уровня в промышленном IoT					
Тема 2. Угрозы и уязвимости сетевого уровня в промышленном IoT		2	4	7	
Раздел 3. Стандарты и нормативные требования по кибербезопасности в IoT					
Тема 3. Стандарты и нормативные требования по кибербезопасности в IoT		2	4	7	
Раздел 4. Методы и инструменты анализа защищённости промышленных сетей					
Тема 4. Методы и инструменты анализа защищённости промышленных сетей		2	4,25	7	
Раздел 5. Проектирование и внедрение систем обнаружения и предотвращения вторжений (IDS/IPS) в IoT					
Тема 5. Проектирование и внедрение систем обнаружения и предотвращения вторжений (IDS/IPS) в IoT		2,25	4,5	7,25	
Раздел 6. Управление рисками и оценка защищённости автоматизированных систем					
Тема 6. Управление рисками и оценка защищённости автоматизированных систем		2	4	7	
Раздел 7. Кибербезопасность при интеграции IoT-устройств в производственные процессы					
Тема 7. Кибербезопасность при интеграции IoT-устройств в производственные процессы		2,25	4,75	7,25	

Раздел 8. Разработка политик и процедур информационной безопасности для промышленных IoT-систем				
Тема 8. Разработка политик и процедур информационной безопасности для промышленных IoT-систем		2,5	4,5	7,25
Итого в семестре (на курсе для ЗАО)		17	34	56,75
Консультации и промежуточная аттестация (Зачет)		0,25		
Всего контактная работа и СР по дисциплине		51,25	56,75	

4 КУРСОВОЕ ПРОЕКТИРОВАНИЕ

Курсовое проектирование учебным планом не предусмотрено

5 БАЛЛЬНО-РЕЙТИНГОВАЯ СИСТЕМА ОЦЕНИВАНИЯ

Использование балльно-рейтинговой системы не предусмотрено.

6. ОПИСАНИЕ ПОКАЗАТЕЛЕЙ, КРИТЕРИЕВ, СИСТЕМЫ И СРЕДСТВ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

6.1 Показатели оценивания

Код компетенции	Показатели оценивания результатов обучения
ПК-3	Способен обосновывать необходимость защиты информации в автоматизированной системе Способен применять знание стандартов IEC 62443, требований ФСТЭК и актуальных угроз для IIoT для выявления каналов утечки и несанкционированного доступа, владеет методиками анализа рисков информационной безопасности, аргументированно обосновывать необходимость внедрения организационных и технических мер защиты с учётом специфики промышленных IoT-систем и последствий реализации угроз.
ПК-7	Способен выбирать технологии и основные компоненты обеспечивающей части создаваемых ИАС Способен применять знание технологий IIoT (MQTT, LoRaWAN, NB-IoT), шлюзов и Edge-вычислений для выбора способа подключения полевых устройств к информационно-аналитической системе (ИАС), владеет навыками проектирования защищённых каналов передачи данных, обосновывать выбор компонентов и технологий с учётом требований производительности, надёжности и информационной безопасности.
ПК-2	Способен контролировать разработку проекта автоматизированной системы управления технологическими процессами Способен применять методы контроля защищённости сетевых подключений для проверки настроек безопасности IIoT-устройств, выявлять несоответствия требованиям, владеет навыками аудита сетевой безопасности, включая анализ конфигураций шлюзов, сегментацию сети и правила фильтрации, обеспечивая соответствие разрабатываемых решений утверждённым требованиям информационной безопасности.

6.2 Система и критерии оценивания

Шкала оценивания	Критерии оценивания сформированности компетенций	
	Устное собеседование	Письменная работа
Зачтено	Студент демонстрирует понимание архитектуры промышленных IoT-систем, основных угроз и уязвимостей сетевого уровня, ключевых стандартов (IEC 62443) и методов оценки рисков. Может обосновать необходимость внедрения конкретных мер защиты (сегментация сети, IDS/IPS, безопасная конфигурация устройств). Способен проанализировать производственный процесс	механосборочного

	производства, выделить этапы для автоматизации и предложить обоснованные решения с учётом экономической эффективности. Допускаются незначительные неточности, не искажающие сути. Речь логична, терминология используется корректно.	
Не зачтено	Студент не может назвать основные угрозы IIoT-сетей, не ориентируется в стандартах ИБ, не способен аргументировать выбор мер защиты. Не различает этапы механосборочного производства, не видит возможностей для автоматизации, не может предложить критерии эффективности. Ответ фрагментарен, отсутствует понимание базовых понятий, терминология не используется или используется ошибочно. Либо ответ отсутствует полностью.	

6.3 Типовые контрольные задания и/или иные материалы, используемые для оценки результатов обучения

6.3.1 Типовые контрольные вопросы

№ п/п	Формулировки вопросов
Семестр 3	
1	Перечислите основные уровни архитектуры промышленного IoT (IIoT) и опишите функции каждого уровня.
2	Назовите три наиболее распространённых протокола IIoT (MQTT, CoAP, AMQP). В чем их преимущества для промышленных систем?
3	Что такое edge-вычисления в контексте IIoT и как они повышают безопасность и отказоустойчивость?
4	Какие типовые угрозы сетевого уровня характерны для IIoT-систем (подмена трафика, DoS, перехват управления, компрометация устройств)?
5	Почему использование протокола MQTT без TLS является уязвимостью? Приведите пример атаки.
6	Назовите основные требования стандарта IEC 62443, применимые к сетевым компонентам IIoT.
7	Какие российские нормативные документы регулируют информационную безопасность объектов КИИ при внедрении IIoT?
8	Сравните активное и пассивное сканирование промышленных сетей. В каком случае предпочтительно пассивное?
9	Какие инструменты (Nmap, OpenVAS, Wireshark) используются для анализа защищённости IIoT-сетей и в чём их назначение?
10	Для чего в IIoT-архитектуре используется DMZ (демилитаризованная зона)? Приведите схему размещения IDS/IPS.
11	Опишите принцип работы сетевой системы обнаружения вторжений (IDS) на примере Snort. В чем отличие IDS от IPS?
12	Назовите этапы управления рисками информационной безопасности для автоматизированной системы на базе IIoT.
13	Как составляется матрица рисков? Какие параметры (вероятность, ущерб, критичность) используются?
14	Перечислите не менее пяти мер безопасной конфигурации IoT-устройства перед интеграцией в производственную сеть.
15	Какие риски возникают при интеграции стороннего IIoT-шлюза в существующую АСУ ТП? Как их минимизировать?
16	Какие разделы должна содержать политика информационной безопасности для промышленной IoT-системы (назовите не менее четырёх).

17	Разработайте план реагирования на инцидент: компрометация IoT-датчика (основные шаги).
18	Опишите структуру механосборочного производства. Какие этапы в нём целесообразно автоматизировать в первую очередь и почему?
19	Как оценить экономическую эффективность внедрения IIoT-решения на механосборочном участке? Назовите основные метрики (OEE, ROI, снижение простоев).
20	Какие методы моделирования и оптимизации производственных процессов (цифровые двойники, имитационное моделирование) применяются при автоматизации механосборочного производства с учётом кибербезопасности?

6.3.2 Типовые тестовые задания

Не предусмотрено.

6.3.3 Типовые практико-ориентированные задания (задачи, кейсы)

1. Выявление угроз и обоснование мер защиты IIoT-сети

На предприятии внедряется система сбора данных с 50 датчиков вибрации через MQTT-брокер. Датчики подключены по Wi-Fi, брокер развёрнут в общей офисной сети. Передача данных — без шифрования.

Задание:

Выявите не менее 3 угроз и уязвимостей в данной конфигурации.

Обоснуйте необходимость внедрения конкретных мер защиты (минимум 3 меры: сетевая сегментация, шифрование, аутентификация устройств).

Составьте краткую пояснительную записку для руководства с рисками и предлагаемыми решениями.

2. Интеграция стороннего IoT-шлюза в АСУ ТП

На механосборочном участке предлагается установить готовый IoT-шлюз (мониторинг энергопотребления станков) стороннего производителя. Шлюз требует доступа к промышленной сети (Modbus TCP) и отправляет данные в облако поставщика.

Задание:

Какие риски несёт подключение стороннего устройства?

Предложите безопасную архитектуру интеграции (сегментация, правила файрвола, диоды данных, ограничения доступа).

Опишите процедуру безопасной настройки шлюза (пароли, сертификаты, отключение неиспользуемых сервисов).

3. Анализ готовности механосборочного участка к автоматизации

Дан участок механосборки: 4 позиции ручной сборки, 2 сварочных робота (работают автономно, без сбора данных), контроль качества — визуальный (оператор). Цель — автоматизация сбора данных о работе оборудования и контроль брака с помощью IIoT-датчиков и компьютерного зрения.

Задание:

Определите «узкие места» и этапы, подлежащие автоматизации в первую очередь.

Оцените ожидаемую экономическую эффективность (не менее 2 показателей: снижение брака, рост производительности).

Назовите требования к кибербезопасности при внедрении IIoT (сегментация, шифрование, обновления).

6.4 Методические материалы, определяющие процедуры оценивания результатов обучения

6.4.1 Условия допуска обучающегося к промежуточной аттестации и порядок ликвидации академической задолженности

Проведение промежуточной аттестации регламентировано локальным нормативным актом СПбГУПТД «Положение о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся»

Положение о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся (принято на Ученом совете университета 15.03.2016г., протокол № 4).

6.4.2 Форма проведения промежуточной аттестации по дисциплине

Устная ☐ + Письменная ☐ Компьютерное тестирование ☐ Иная ☐

6.4.3 Особенности проведения промежуточной аттестации по дисциплине

- ☐ Возможность пользоваться справочными материалами, калькулятором;
- ☐ Время на подготовку ответа на зачете -30 минут.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

7.1 Учебная литература

Автор	Заглавие	Издательство	Год издания	Ссылка
7.1.1 Основная учебная литература				

Страшун, Ю. П.	Технические средства автоматизации и управления	Москва: Издательский Дом МИСиС	2015	http://www.iprbookshop.ru/98894.html
7.1.2 Дополнительная учебная литература				
Белоус, А. И.	Кибербезопасность объектов топливно- энергетического комплекса. Концепции, методы и средства обеспечения	Москва, Вологда: Инфра-Инженерия	2020	http://www.iprbookshop.ru/98348.html
Белоус, А. И., Солодуха, В. А.	Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения	Москва: Техносфера	2021	https://www.iprbookshop.ru/108023.html

7.2 Перечень профессиональных баз данных и информационно-справочных систем

1. Электронная библиотека СПб ГУПТД - <http://www.iprbookshop.ru>.
2. Электронная библиотека ВШТЭ СПб ГУПТД - http://nizrp.narod.ru/ebmu_m.htm.

7.3 Перечень лицензионного и свободно распространяемого программного обеспечения

MicrosoftWindows 8

MicrosoftOfficeProfessional 2013

7.4 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

1. Лекционная аудитория с мультимедийным учебным комплексом
2. Компьютерный класс с мультимедийным комплексом и выходом в Интернет