

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.ДВ.01.02 Тестирование и кибербезопасность промышленного программного обеспечения

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	Лаб. занятия				
2	УП	17	34	57	36	4	Экзамен
	РПД	17	34	57	36	4	
Итого	УП	17	34	57	36	4	
	РПД	17	34	57	36	4	

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 тестирования и обеспечения кибербезопасности промышленного программного обеспечения, используемого в автоматизированных системах управления технологическими процессами (АСУ ТП).

1.2 Задачи дисциплины:

- Изучить основные принципы и методы тестирования промышленного программного обеспечения, включая функциональное, нагрузочное, интеграционное и регрессионное тестирование.
- Ознакомить с современными инструментами и технологиями автоматизации тестирования в сфере АСУ ТП.
- Сформировать понимание специфики кибербезопасности в промышленных информационных системах, включая анализ угроз и уязвимостей.
- Научить применять методы и средства защиты информации, соответствующие требованиям законодательства и отраслевым стандартам.
- Развить навыки проектирования и реализации тестовых сценариев для выявления ошибок и уязвимостей в программном обеспечении АСУ ТП.

1.3 Требования к предварительной подготовке обучающегося:

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

знание основ информационной безопасности и организации систем управления АСУ ТП

2 КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ПК-7: Способен выбирать технологии и основные компоненты обеспечивающей части создаваемых ИАС
Знать: - современные технологии тестирования и обеспечения кибербезопасности промышленного программного обеспечения; - основные компоненты и архитектуру обеспечивающей части ИАС в сфере автоматизированных систем управления технологическими процессами (АСУ ТП); - требования к выбору технологий и инструментов для тестирования и защиты информации в промышленных ИАС; - методы анализа и оценки уязвимостей программного обеспечения, используемого в АСУ ТП;
Уметь: - анализировать задачи и условия эксплуатации ИАС для обоснованного выбора технологий и компонентов обеспечивающей части; - подбирать и применять современные инструменты тестирования и средства защиты информации для промышленных ИАС; - оценивать соответствие выбранных технологий требованиям безопасности, надёжности и эффективности; - разрабатывать и реализовывать тестовые сценарии для проверки функциональности и защищённости компонентов ИАС;
Владеть: - навыками выбора и интеграции технологий тестирования и кибербезопасности в структуру промышленных ИАС; - методами проектирования и реализации обеспечивающей части ИАС с учётом требований к тестированию и информационной безопасности; - практическими умениями по применению инструментов автоматизации тестирования и средств защиты информации в АСУ ТП;

3 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Наименование и содержание разделов, тем и учебных занятий	Семестр (курс для ЗАО)	Контактная работа		СР (часы)	Форма текущего контроля
		Лек. (часы)	Лаб. (часы)		
Раздел 1. Особенности тестирования программного обеспечения АСУ ТП: методы, инструменты и стандарты.	2				
Тема 1. Введение в тестирование и кибербезопасность промышленного ПО		2	4	7	
Раздел 2. Кибербезопасность промышленных информационных систем: анализ угроз и уязвимостей.					
Тема 2. Современные методы и инструменты тестирования промышленного ПО		2	4	7	
Раздел 3. Функциональное и нагрузочное тестирование компонентов ИАС в автоматизированных производствах.					
Тема 3. Уязвимости и методы их выявления в АСУ ТП		2	4	7	
Раздел 4. Интеграционное тестирование и верификация данных в распределённых АСУ ТП.					
Тема 4. Статический и динамический анализ кода в промышленных системах		2	4,5	7,5	
Раздел 5. Методы и средства защиты информации в промышленных сетях и SCADA-системах.					
Тема 5. Тестирование на проникновение (пентест) АСУ ТП		2	4,5	7,5	
Раздел 6. Автоматизация тестирования и аудита безопасности промышленного ПО.					
Тема 6. Обеспечение безопасности жизненного цикла разработки ПО (DevSecOps) для промышленных систем		2,5	4,5	7,5	
Раздел 7. Реагирование на инциденты кибербезопасности и восстановление работоспособности АСУ ТП.					

Тема 7. Анализ защищённости и управление уязвимостями в АСУ ТП		2,5	4,5	7	
Раздел 8. Нормативно-правовое регулирование и отраслевые стандарты тестирования и кибербезопасности в промышленности.					
Тема 8. Оценка соответствия и сертификация промышленного ПО по требованиям безопасности		2	4	6,5	
Итого в семестре (на курсе для ЗАО)		17	34	57	
Консультации и промежуточная аттестация (Экзамен)		2,5		33,5	
Всего контактная работа и СР по дисциплине		53,5		90,5	

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-7	Способен анализировать задачи и условия эксплуатации информационно-аналитических систем (ИАС) для обоснованного выбора технологий и компонентов обеспечивающей части в сфере АСУ ТП, подбирать и применять современные инструменты тестирования и средства защиты информации для промышленных ИАС, оценивать соответствие выбранных технологий требованиям безопасности, надёжности и эффективности, разрабатывать и реализовывать тестовые сценарии для проверки функциональности и защищённости компонентов, владеет навыками выбора и интеграции технологий тестирования и кибербезопасности в структуру промышленных ИАС, методами проектирования и реализации обеспечивающей части ИАС с учётом требований к тестированию и информационной безопасности, практическими умениями по применению инструментов автоматизации тестирования и средств защиты информации в АСУ ТП.

6.2 Система и критерии оценивания

Шкала оценивания	Критерии оценивания сформированности компетенций	
	Устное собеседование	Письменная работа
5 (отлично)	Студент демонстрирует глубокое понимание современных технологий тестирования и кибербезопасности промышленного ПО, архитектуры обеспечивающей части ИАС, методов анализа уязвимостей. Свободно обосновывает выбор инструментов тестирования и средств защиты для конкретных условий эксплуатации АСУ ТП. Приводит примеры из реальной практики (конкретные инструменты, типы тестов, сценарии атак). Разрабатывает тестовые сценарии и оценивает эффективность защиты. Ответ логичен, терминология безупречна.	Письменная работа выполнена полностью и без ошибок. Студент правильно определяет задачи тестирования и кибербезопасности, обоснованно выбирает инструменты (например, статический анализатор кода, fuzzing-средства, сканер уязвимостей) для заданной ИАС. Разрабатывает тестовые сценарии, оценивает риски. Оформление соответствует требованиям.
4 (хорошо)	Студент владеет материалом, но допускает незначительные неточности	Работа выполнена в полном объёме, но содержит 1–2 неточности (например, не

	(например, неполное описание этапов тестирования, путаница в двух смежных инструментах). Обоснование выбора в целом верное, но недостаточно развёрнутое. Примеры приводит, но носят общий характер. На дополнительные вопросы отвечает с небольшими подсказками.	указан конкретный инструмент автоматизации, не полностью описана процедура оценки уязвимостей). Обоснования в целом верные, но недостаточно детальные.
3 (удовлетворительно)	Студент демонстрирует минимально достаточный уровень: знает базовые понятия тестирования и кибербезопасности, но не может обосновать выбор инструментов или методов. Путается в типах тестов (функциональное, нагрузочное, пентест). Не может оценить соответствие требованиям безопасности. Речь фрагментарна, терминология используется неточно.	Работа выполнена частично (не менее 60%). Допущены содержательные ошибки в выборе методов или инструментов тестирования. Основные компетенции в целом узнаваемы, но решение не полностью обосновано.
2 (неудовлетворительно)	Студент не владеет материалом. Не может назвать ни одного метода тестирования или средства защиты промышленного ПО. Не понимает архитектуры ИАС. Ответ отсутствует или полностью не по теме.	Работа выполнена менее чем на 60%, либо содержит грубые ошибки (не различает виды тестирования, выбирает несовместимые компоненты, игнорирует требования безопасности). Решение отсутствует или полностью неверное.

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 2	
1	Дайте определение понятиям «safety» и «security» применительно к промышленному ПО. Чем они отличаются и как связаны?
2	Назовите основные этапы жизненного цикла разработки промышленного ПО по стандарту IEC 62443-4-1.
3	Чем тестирование промышленного ПО отличается от тестирования обычного корпоративного ПО?
4	Какие виды тестирования (функциональное, нагрузочное, стресс-тестирование, отказоустойчивость) применяются для АСУ ТП? Опишите их.
5	Приведите примеры типовых уязвимостей промышленного ПО (буферы, небезопасные функции, отсутствие аутентификации, жестко зашитые пароли).
6	Что такое CVE? Как найти уязвимости, характерные для SCADA или ПЛК?
7	Какие инструменты статического анализа кода (линтеры, анализаторы) могут использоваться для языков программирования ПЛК (ST, FBD, C++)?
8	В чем разница между статическим и динамическим анализом кода? Приведите примеры.
9	Что такое fuzzing (фаззинг) и как он применяется для поиска уязвимостей в промышленных протоколах?
10	Опишите этапы пентеста АСУ ТП (сбор информации, сканирование, эксплуатация, пост-эксплуатация).
11	Какие ограничения и меры предосторожности необходимо соблюдать при проведении пентеста на работающем промышленном объекте?
12	Что такое DevSecOps? Как интегрировать безопасность в CI/CD пайплайн для промышленного ПО?
13	Какие требования к безопасному кодированию предъявляет стандарт IEC 62443-4-1?

14	Как организуется управление уязвимостями в АСУ ТП (идентификация, классификация, приоритизация, устранение)? Назовите популярные базы уязвимостей (CVE, NVD, ICS-CERT). Какую информацию они содержат? Какие автоматизированные системы сканирования уязвимостей (например, MaxPatrol, Security Code Scanner) могут применяться для промышленного ПО?
15	Какие нормативные документы РФ регулируют требования к безопасности промышленного ПО для объектов КИИ (приказы ФСТЭК)?
16	Опишите процедуру сертификации промышленного ПО по требованиям информационной безопасности.
17	Какие разделы документации необходимо подготовить для сертификации промышленного ПО?
18	Что такое модель угроз для промышленного ПО и как она используется при тестировании на проникновение?

6.3.2 Типовые тестовые задания

Не предусмотрено.

6.3.3 Типовые практико-ориентированные задания (задачи, кейсы)

1. Тестирование на отказоустойчивость ПЛК

На стенде установлен ПЛК Siemens S7-1200, который управляет температурой в печи. Требуется проверить, как устройство поведёт себя при аномальных входных данных (выход за границы диапазона, быстрое изменение, отсутствие сигнала).

Задание:

Разработайте сценарии нефункционального тестирования (3 варианта).

Опишите, как будете генерировать тестовые воздействия.

Какие параметры будете мониторить (температура, состояние регулятора, сообщения об ошибках)?

Дайте рекомендации по повышению отказоустойчивости.

2. Пентест Modbus TCP

В лабораторной среде имеется эмулятор ПЛК с поддержкой Modbus TCP (стандартные порт 502). Необходимо выявить уязвимости и оценить возможность несанкционированного управления.

Задание:

Используя Nmap, определите открытые порты и сервисы.

С помощью специальных скриптов (например, modbus-discover) найдите доступные функции и регистры.

Попробуйте изменить значение удерживающего регистра (например, команду запуска двигателя).

Составьте отчет о найденных уязвимостях (отсутствие аутентификации, возможность записи).

Предложите меры защиты (firewall, VPN, аутентификация, сегментация).

3. Внедрение DevSecOps в промышленную компанию

Предприятие разрабатывает собственное ПО для SCADA. Разработка ведётся без систем контроля версий, тестирование – только ручное перед релизом.

Задание:

Предложите поэтапный план перехода на DevSecOps (инструменты, процессы).

Какие автоматизированные тесты (модульные, интеграционные, безопасности) вы включите в CI/CD?

Как организовать статический анализ кода и проверку уязвимостей зависимостей?

Оцените бюджет времени и возможные риски при внедрении.

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

Время на подготовку ответа - 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				
Белоус, А. И., Солодуха, В. А.	Кибероружие и кибербезопасность. О сложных вещах простыми словами	Москва, Вологда: Инфра-Инженерия	2020	http://www.iprbookshop.ru/98349.html
7.1.2 Дополнительная учебная литература				
Кудяров, Ю. А.	Испытания (тестирование) программного обеспечения средств измерений	Москва: Академия стандартизации, метрологии и сертификации	2010	http://www.iprbookshop.ru/44241.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