

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.01.01 Информационная безопасность АСУ ТП

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, умений и навыков, необходимых для обеспечения комплексной защиты автоматизированных систем управления технологическими процессами от современных киберугроз. Дисциплина направлена на подготовку специалистов, способных анализировать, проектировать и внедрять эффективные меры по обеспечению информационной безопасности в сфере автоматизации производств.

1.2 Задачи дисциплины:

- Изучить основные понятия, принципы и стандарты информационной безопасности применительно к АСУ ТП.
- Освоить методы анализа угроз и уязвимостей, характерных для промышленных информационных систем.
- Сформировать навыки проектирования и внедрения систем защиты информации в автоматизированных производствах.
- Научиться применять современные средства и технологии для обеспечения конфиденциальности, целостности и доступности данных в АСУ ТП.
- Развить умение оценивать риски информационной безопасности и разрабатывать мероприятия по их минимизации.

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

2 КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ПК-7: Способен выбирать технологии и основные компоненты обеспечивающей части создаваемых ИАС
Знать: - Основные технологии и компоненты, используемые в обеспечивающей части информационных аналитических систем (ИАС) для АСУ ТП. - Принципы построения и функционирования обеспечивающей части ИАС, включая архитектуру, программное и аппаратное обеспечение. - Требования к информационной безопасности при выборе технологий и компонентов для ИАС в АСУ ТП. - Современные стандарты и нормативные документы, регламентирующие выбор компонентов и технологий для ИАС в сфере автоматизации технологических процессов. - Методы оценки и сравнения различных технологий и компонентов по критериям надёжности, защищённости, масштабируемости и совместимости.
Уметь: - Анализировать задачи автоматизации и информационной безопасности для обоснованного выбора технологий и компонентов ИАС. - Подбирать и обосновывать использование конкретных программных и аппаратных средств для построения обеспечивающей части ИАС. - Проводить сравнительный анализ различных технологических решений по критериям информационной безопасности и эффективности. - Разрабатывать технические задания и спецификации на компоненты обеспечивающей части ИАС с учётом требований безопасности.
Владеть: - Навыками выбора и обоснования технологий и компонентов обеспечивающей части ИАС для АСУ ТП с учётом требований информационной безопасности. - Методиками проектирования и документирования обеспечивающей части ИАС, включая описание архитектуры, состава и взаимодействия компонентов. - Практическими умениями по интеграции и настройке выбранных компонентов в составе ИАС для автоматизированных систем управления технологическими процессами. - Способностью оценивать риски и принимать решения по выбору технологий на основе анализа угроз и уязвимостей.

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. Анализ угроз и уязвимостей в современных АСУ ТП	2				
Тема 1. Классификация угроз, примеры атак, методы выявления уязвимостей.		2	4	7	
Раздел 2. Архитектура и компоненты обеспечивающей части информационных аналитических систем (ИАС) для АСУ ТП					
Тема 2. Выбор технологий, интеграция компонентов, требования к безопасности.		2	4	7	
Раздел 3. Методы и средства защиты информации в автоматизированных системах управления технологическими процессами					
Тема 3. Программные и аппаратные средства, криптографические методы, контроль доступа.		2	4	7	
Раздел 4. Нормативно-правовое регулирование информационной безопасности АСУ ТП в России					
Тема 4. Стандарты, законы, отраслевые требования, сертификация.		2	4,5	7,5	
Раздел 5. Организация мониторинга и реагирования на инциденты информационной безопасности в АСУ ТП					
Тема 5. Построение систем мониторинга, анализ событий, алгоритмы реагирования.		2	4,5	7,5	
Раздел 6. Безопасность сетевой инфраструктуры АСУ ТП					
Тема 6. Защита промышленных протоколов, сегментация сетей, межсетевые экраны.		2,5	4,5	7	
Раздел 7. Обеспечение информационной безопасности при интеграции АСУ ТП с корпоративными информационными системами					

Тема 7. Риски интеграции, методы защиты, примеры проектных решений.		2,5	4,5	7	
Раздел 8. Практические аспекты внедрения и эксплуатации систем защиты информации в АСУ ТП					
Тема 8. Этапы внедрения, обучение персонала, аудит и оценка эффективности.		2	4	7	
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 автоматизации и информационной безопасности для обоснованного выбора технологий и компонентов информационно-аналитических систем (ИАС) в составе АСУ ТП, подбирать и обосновывать использование конкретных программных и аппаратных средств (серверы, СУБД, платформы визуализации, средства интеграции, защиты информации), проводить сравнительный анализ технологических решений по критериям надёжности, защищённости, масштабируемости и совместимости, разрабатывать технические задания и спецификации с учётом требований безопасности, владеет навыками проектирования и документирования обеспечивающей части ИАС, практическими умениями по интеграции и настройке выбранных компонентов, способен оценивать риски и принимать решения на основе анализа угроз и уязвимостей.

6.2 Система и критерии оценивания

Шкала оценивания	Критерии оценивания сформированности компетенций	
	Устное собеседование	Письменная работа
5 (отлично)	Студент демонстрирует глубокое системное понимание технологий и компонентов обеспечивающей части ИАС для АСУ ТП. Свободно ориентируется в принципах построения архитектуры, критериях выбора (надёжность, защищённость, масштабируемость, совместимость). Обоснованно сравнивает альтернативные решения, учитывая требования информационной безопасности. Приводит примеры из реальной практики (конкретные СУБД, платформы, средства защиты). Аргументирует выбор компонентов для заданного сценария. Ответ логичен, развёрнут, терминология безупречна. Уверенно отвечает на дополнительные и уточняющие вопросы.	Письменная работа выполнена полностью и без ошибок. Студент правильно определяет тип задач автоматизации, обоснованно выбирает компоненты ИАС (аппаратные, программные, сетевые) с учётом требований информационной безопасности. В кейсе – чёткая аргументация выбора, сравнение альтернатив по заданным критериям (стоимость, производительность, надёжность, защищённость). Оформление соответствует требованиям (спецификации, техническое задание).
4 (хорошо)	Студент владеет основным	Работа выполнена в полном объёме, но

	материалом, но допускает незначительные неточности (например, неполное перечисление критериев, путаница в двух смежных технологиях). Обоснование выбора в целом верное, но недостаточно развёрнутое. Примеры приводит, но носят общий или учебный характер. На дополнительные вопросы отвечает, но с небольшими подсказками. Терминология в основном корректна.	содержит 1–2 негрубые ошибки (например, не указан конкретный стандарт, не полностью описана архитектура). Обоснования в целом верные, но недостаточно детальные. В кейсе решение правильное, но часть шагов выполнена без развёрнутого пояснения.
3 (удовлетворительно)	Студент демонстрирует минимально достаточный уровень. Знает базовые компоненты ИАС, но не может обосновать их выбор. Путается в критериях оценки, не различает требования надёжности и защищённости. Примеров не приводит или они не относятся к делу. На дополнительные вопросы отвечает с трудом, требуется значительная помощь. Речь фрагментарна, терминология используется неточно.	Работа выполнена частично (не менее 60% объёма). Допущены содержательные ошибки в выборе компонентов или критериях. Например, выбран сервер без учёта требований к отказоустойчивости, или не учтены требования ИБ. Основные компетенции в целом узнаваемы, но решение не полностью обосновано.
2 (неудовлетворительно)	Студент не владеет материалом. Не может назвать ни одного компонента ИАС, не понимает принципов выбора технологий. Не ориентируется в требованиях информационной безопасности. Ответ отсутствует, полностью не по теме, либо демонстрирует полное непонимание предмета.	Работа выполнена менее чем на 60%, либо содержит грубые принципиальные ошибки (не различает СУБД и SCADA, выбирает несовместимые компоненты, игнорирует требования безопасности). Решение отсутствует или полностью неверное. Оформление отсутствует или нечитаемо.

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 понятия «угроза информационной безопасности» применительно к АСУ ТП. Чем угрозы для АСУ ТП отличаются от угроз для офисных ИТ-систем?
2	Приведите классификацию угроз информационной безопасности в АСУ ТП (естественные, случайные, преднамеренные). Приведите по 2 примера каждого типа.
3	Назовите не менее трёх известных кибератак на АСУ ТП (Stuxnet, Havex, BlackEnergy). Кратко опишите механизм и последствия каждой.
4	Какие методы выявления уязвимостей применяются при анализе защищённости АСУ ТП (сканирование, пентест, анализ конфигураций)? В чём особенности их применения в промышленных сетях?
5	Перечислите основные компоненты обеспечивающей части информационно-аналитической системы (ИАС) в составе АСУ ТП. Назовите критерии выбора этих компонентов с учётом требований безопасности.
6	По каким критериям (надёжность, защищённость, масштабируемость, совместимость) оцениваются технологии и компоненты ИАС для АСУ ТП? Раскройте каждый критерий.
7	Назовите основные программные и аппаратные средства защиты информации в АСУ ТП (антивирусы, межсетевые экраны, диоды данных, SIEM, DLP).
8	Какие криптографические методы применяются для защиты данных в АСУ ТП (шифрование каналов, электронная подпись, VPN)? В чём сложность их внедрения на промышленных объектах?
9	Что такое системы контроля доступа (RBAC, MAC)? Как они реализуются в АСУ ТП на уровне SCADA и ПЛК?

10	Перечислите основные нормативные правовые акты РФ, регулирующие информационную безопасность АСУ ТП (152-ФЗ, 187-ФЗ, 259-ФЗ, приказы ФСТЭК).
11	Какие требования предъявляет приказ ФСТЭК №239 к системам защиты информации объектов КИИ? Назовите основные меры.
12	Что такое стандарт IEC 62443? Какие его части наиболее актуальны для АСУ ТП и почему?
13	Как строится система мониторинга информационной безопасности в АСУ ТП? Какие компоненты (SIEM, IDS/IPS) используются и как они взаимодействуют?
14	Опишите алгоритм реагирования на инцидент информационной безопасности в АСУ ТП (обнаружение, локализация, устранение, восстановление).
15	В чем особенности защиты промышленных протоколов (Modbus, Profinet, DNP3)? Какие уязвимости им присущи и как их минимизировать?
16	Что такое сегментация сети АСУ ТП? Как выделяются зоны безопасности (DMZ, control zone, field zone) и какие правила фильтрации на границах?
17	Какие риски возникают при интеграции АСУ ТП с корпоративными информационными системами (ERP, MES, BI)? Назовите типовые угрозы.
18	Опишите типовую схему безопасной интеграции промышленной сети с офисной сетью (industrial DMZ). Какие устройства размещаются в DMZ?
19	Перечислите основные этапы внедрения системы защиты информации на объекте АСУ ТП (от обследования до ввода в эксплуатацию). Какие документы разрабатываются?
20	Как оценивается эффективность системы защиты информации в АСУ ТП? Назовите не менее трёх метрик (показателей) эффективности.

6.3.2 Типовые тестовые задания

Не предусмотрено.

6.3.3 Типовые практико-ориентированные задания (задачи, кейсы)

1. Анализ угроз и выбор мер защиты

На предприятии АСУ ТП имеет архитектуру: ПЛК Siemens S7 (Modbus TCP), SCADA на базе WinCC, соединённые через неуправляемый коммутатор. Есть удалённый доступ через RDP для вендора.

Задание: Выявить не менее 4 угроз. Предложить меры защиты (сегментация, firewall, шифрование, управление доступом). Кратко обосновать.

2. Разработка политики реагирования на инцидент

На SCADA-сервере обнаружена аномальная активность (подозрительный процесс, исходящие соединения на внешний IP).

Задание: Опишите пошаговый план реагирования (обнаружение, локализация, устранение, восстановление, анализ). Укажите, кого уведомить и какие данные сохранить.

3. Оценка безопасности сетевой интеграции

Технологическая сеть (Modbus TCP) соединяется с корпоративной сетью (ERP) через неуправляемый маршрутизатор без фильтрации.

Задание: Укажите 3 риска. Предложите безопасную архитектуру сопряжения с использованием industrial DMZ и межсетевого экрана с глубокой фильтрацией пакетов. Нарисуйте схему

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				
Жук А.П., Жук Е.П., Лепешкин О.М. и др.	Защита информации	Москва: ИЦ РИО	2021	https://ibooks.ru/reading.php?short=1&productid=361250
Фомин, Д. В.	Защита информации: специализированные аттестованные программные и программно-аппаратные средства	Саратов: Вузовское образование	2021	http://www.iprbookshop.ru/110329.html
7.1.2 Дополнительная учебная литература				
С.Л. Морева	Защита информации : практикум	М-во науки и высшего образования РФ, С.-Петерб. гос. ун-т пром. технологий и дизайна, Высш. шк. технологии и энергетики. - Санкт-Петербург : ВШТЭ СПбГУПТД	2020	http://nizrp.narod.ru/metod/kafinfizmtex/1632862450.pdf

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