ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Руководитель специальности

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Соколов А. Н.
Пользователь: sokolovan
Дата подписания: 04.09.2024

А. Н. Соколов

РАБОЧАЯ ПРОГРАММА

дисциплины 1.Ф.09 Кибербезопасность интеллектуальных автоматизированных систем управления технологическими процессами
для специальности 10.05.03 Информационная безопасность автоматизированных систем
уровень Специалитет
форма обучения очная
кафедра-разработчик Защита информации

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем, утверждённым приказом Минобрнауки от 26.11.2020 № 1457

Зав.кафедрой разработчика,
к.техн.н., доц.

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Соколов А. Н.
Пользователь: sokolovan
Дата подписания: 04.09.2024

А. Н. Соколов

Разработчик программы,
старший преподаватель

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Баринов А. Е.
Пользователь: barinovae
Дата подписания: 03.09.2024

А. Е. Баринов

Челябинск

1. Цели и задачи дисциплины

Целью изучения дисциплины является приобретение знаний о проблемах обеспечения кибербезопасности в критических системах и навыков, которые необходимы при работе по обеспечению информационной безопасности АСУ ТП на критических объектах. Дисциплина включает материалы, лежащие на стыке двух отраслей: информационная безопасность и автоматизация производств.

Краткое содержание дисциплины

В курсе рассматриваются типовые архитектуры АСУ ТП, угрозы, уязвимости и атаки на АСУ ТП. Основы функциональной безопасности. В качестве прикладных аспектов информационной безопасности основное внимание уделяется защите изолированных сетей, организации DMZ, изучение спецеиализированного вредоносного ПО и методов противодействия ему.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине
ПК-1 Способен моделировать защищенные автоматизированные системы с целью анализа их уязвимостей и эффективности средств и способов защиты информации	Знает: уязвимости современных АСУ ТП, подходы к устранению уязвимостей и построению системы защиты современных АСУ ТП Умеет: анализировать структуры АСУ ТП, строить их модели, оценивать риски функциональной безопасности, распознавать атаки социальной инженерии Имеет практический опыт: разработки политик безопасности современных промышленных систем автоматизации, исследования сетевых пакетов в промышленной сети
ПК-4 Способен разрабатывать организационно-распорядительные документы и внедрять организационные меры по защите информации в автоматизированных системах	Знает: нормативные документы Российской федерации в области кибербезопасности; особенности организации подразделения центра управления инцидентами (ЦУИ ИБ) для поддержки информационной безопасности промышленной сети
ПК-5 Способен выполнять работы по администрированию систем защиты информации автоматизированных систем и обеспечивать их работоспособность при возникновении нештатных ситуаций	Знает: архитектуру автоматизированной системы управления технологическим процессом (АСУ ТП), модели промышленных систем автоматизации, сетевые технологии, используемые в современных АСУ ТП, понятия функциональной и информационной безопасности, их взаимосвязь и противоречия; основы организации своевременной и полноценной обработки инцидентов безопасности Умеет: работать со средствами обеспечения безопасности в системах промышленной автоматизации; настраивать межсетевой экран для обеспечения защиты периметра сети, для

	обеспечения сегментации внутренней сети Имеет практический опыт: анализа инцидентов кибербезопасности в современных промышленных системах автоматизации

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
1.Ф.01 Автоматизированные системы управления, 1.Ф.02 Современные киберугрозы в промышленных и корпоративных системах автоматизации, 1.Ф.04 Защита информации в сети Интернет, 1.Ф.05 Кодирование информации в автоматизированных системах управления	Не предусмотрены

Требования к «входным» знаниям, умениям, навыкам студента, необходимым при освоении данной дисциплины и приобретенным в результате освоения предшествующих дисциплин:

Дисциплина	Требования
1.Ф.01 Автоматизированные системы управления	Знает: архитектуру промышленных сетей АСУ ТП, цели и задачи автоматизации управления, общие понятия автоматизированных систем управления (АСУ), жизненный цикл, функции и виды АСУ;состав автоматизированных систем управления технологическим процессом (АСУ ТП), виды обеспечения, классификацию и уровни управления АСУ ТП, место АСУ ТП в интегрированных системах управления Умеет: применять методы и средства регистрации, записи и хранения значимых параметров потоков данных АСУ ТП, анализировать и моделировать информационные процессы, протекающие в системах промышленной автоматизации Имеет практический опыт: определения ключевых точек мониторинга значимых параметров потоков данных, распределенных в информационной системе промышленных сетей АСУ ТП
1.Ф.02 Современные киберугрозы в промышленных и корпоративных системах автоматизации	Знает: актуальные угрозы информационной безопасности промышленных компаний, текущее состояние и эволюцию киберугроз как ответную реакцию на внедрение средств и мер информационной безопасности, типы современных киберугроз в промышленных и корпоративных системах автоматизации, актуальные векторы атак на промышленные сети АСУ ТП;средства и меры информационной безопасности, применяемые в промышленных и корпоративных системах автоматизации Умеет: анализировать и оценивать риски

	информационной безопасности в промышленных и корпоративных системах автоматизации, проводить аналитику современных киберугроз в промышленных и корпоративных системах автоматизации, актуальные векторы атак на промышленные сети АСУ ТП Имеет практический опыт: идентификации и моделирования каналов возможного деструктивного информационно-технического воздействия в промышленных и корпоративных системах автоматизации, оценки уязвимостей по отношению к современным киберугрозам промышленных сетей АСУ ТП
1.Ф.04 Защита информации в сети Интернет	Знает: основные направления защиты информации в информационно-телекоммуникационных системах в соответствии с законодательством Российской Федерации;современные технологии защиты от вредоносного программного обеспечения, распространяемого по сети Интернет Умеет: проводить оценку угроз безопасности информационно-телекоммуникационной системы, подключенной к сети Интернет;реализовывать технологии защиты от вредоносного программного обеспечения, распространяемого по сети Интернет Имеет практический опыт: использования антивирусного программного обеспечения для защиты информации в информационно-телекоммуникационных системах, подключенных к сети Интернет
1.Ф.05 Кодирование информации в автоматизированных системах управления	Знает: основные способы кодирования информации в автоматизированных системах управления (АСУ), обеспечивающие максимальную надежность и высокую скорость при ее передаче по каналам связи (коды: линейные, циклические, БЧХ, Хэмминга, Шеннона - Фано и Хаффмана) Умеет: решать типовые задачи кодирования и декодирования информации с использованием математических методов и моделей Имеет практический опыт: применения помехоустойчивых шифров и кодов, повышающих скорость передачи информации в АСУ

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 4 з.е., 144 ч., 70,5 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра

		11
Общая трудоёмкость дисциплины	144	144
Аудиторные занятия:	60	60
Лекции (Л)	24	24
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	24	24
Лабораторные работы (ЛР)	12	12
Самостоятельная работа (СРС)	73,5	73,5
Объект исследования – интеллектуальная АСУ ТП	6	6
Проблема обеспечения кибербезопасности АСУ ТП	6	6
Социальная инженерия	6	6
Защита изолированных сетей	6	6
Атаки на интеллектуальные АСУ ТП	6	6
Введение	5	5
Типовое вредоносное ПО АСУ ТП	10,5	10.5
Организация подразделения обеспечения промышленной кибербезопасности. Политика безопасности	6	6
Функциональная безопасность АСУ ТП	6	6
Безопасность сетей АСУ ТП	16	16
Консультации и промежуточная аттестация	10,5	10,5
Вид контроля (зачет, диф.зачет, экзамен)	-	экзамен

5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах			
		Всего	Л	ПЗ	ЛР
1	Введение	2	2	0	0
2	Объект исследования – интеллектуальная АСУ ТП	4	2	2	0
3	Функциональная безопасность АСУ ТП	4	2	2	0
4	Проблема обеспечения кибербезопасности АСУ ТП	10	4	4	2
5	Атаки на интеллектуальные АСУ ТП	6	2	2	2
6	Безопасность сетей АСУ ТП	10	2	4	4
7	Защита изолированных сетей	8	4	2	2
8	Социальная инженерия	6	2	4	0
9	Типовое вредоносное ПО АСУ ТП	6	2	2	2
10	Организация подразделения обеспечения промышленной кибербезопасности. Политика безопасности	4	2	2	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Эволюция АСУ ТП Технологии современных АСУ ТП	2
2	2	Основные определения в области промышленной автоматизации. Модель промышленной системы по ФСТЭК. Модель промышленной системы PERA	2
4	3	Функциональная безопасность в АСУ ТП. Функциональная и информационная безопасность. Их взаимосвязь и противоречие. Дерево сбоев и атак. Единая модель.	2

5	4	Нормативные документы Российской федерации в области кибербезопасности. 31 приказ ФСТЭК и другие документы Федеральный закон 187 Международные нормативные документы. Документы NERC CIP, NIST Понятие эшелонированной защиты. Трудности при внедрении эшелонированной защиты.	2
6	4	Проблемы обеспечения безопасности современных промышленных систем. Атаки на современные промышленные системы – общие положения. Уязвимости современных промышленных системы – причины. Устранение уязвимостей. Обновление программного обеспечения промышленных систем. Проблемы устранения уязвимостей и способы их решения. Отличительные особенности и проблемы обеспечения методов обеспечения кибербезопасности промышленных предприятий. Угрозы информационной безопасности в АСУ ТП. Объекты защиты АСУ ТП	2
7	5	Типовая схема вторжения. Атаки на сети промышленных систем. Сканирование сетевых систем. Средства сканирования сетевых систем.	2
9	6	Обзор протоколов сетей АСУ ТП. Принципы работы и вопросы безопасности	2
11	7	Понятие «воздушного зазора». Способы атак на промышленные системы, не подключенные к сети Интернет. Преодоление «воздушного зазора». Сменные носители. Политика использования сменных носителей Атака со стороны поставщиков и внутренних нарушителей. Методы защиты от атак со стороны поставщиков и внутренних нарушителей.	2
12	7	Угрозы и защита беспроводных коммуникаций в сетях АСУ ТП. Удаленный доступ и его защита.	2
13	8	Фишинг с использованием электронной почты. Признаки фишинга. Направленный фишинг. Фишинг с использованием социальных сетей.	2
14	9	Разбор известных инцидентов атаки промышленных систем посредством вредоносного ПО.	2
16	10	Подразделение ИБ АСУ ТП. Особенности организации работы. Задачи подразделения кибербезопасности. Взаимодействие с другими структурами	2

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	2	Анализ структур различных АСУ ТП	2
2	3	Рассмотрение моделей и расчёт рисков функциональной безопасности	2
3	4	Анализ проблем защищённости и выработка требований к защите типовых АСУ ТП	4
4	5	Модель атаки и нарушителя АСУ ТП	2
5	6	Разбор протоколов сетей АСУ ТП	2
6	6	Подходы по интеграции в сеть АСУ ТП защитных решений	2
7	7	Обсуждение проблематики "воздушного зазора"	2
9	8	Рассмотрение подходов различных видов социальной инженерии	2
10	8	Программы повышения осведомлённости сотрудников	2
11	9	Обзор типового вредоносного ПО АСУ ТП	2
12	10	Деловая игра по формированию подразделения ИБ АСУ ТП	2

5.3. Лабораторные работы

№ занятия	№ раздела	Наименование или краткое содержание лабораторной работы	Кол-во

			часов
1	4	Изучение дампов сетевого трафика промышленных протоколов	2
2	5	Обнаружение и исследование уязвимостей промышленных устройств	2
3	6	Сегментация промышленных сетей	2
4	6	Настройка IDS для промышленной сети	2
5	7	Расширенная настройка правил сетевой безопасности для обнаружения целевых атак	2
6	9	Настройка средств обеспечения ИБ уровня конечного узла	2

5.4. Самостоятельная работа студента

Выполнение СРС			
Подвид СРС	Список литературы (с указанием разделов, глав, страниц) / ссылка на ресурс	Семестр	Кол-во часов
Объект исследования – интеллектуальная АСУ ТП	Основы кибербезопасности интеллектуальных энергосистем : Учебный курс для магистров / Семён Корт — Лаборатория Касперского, 2019 (в локальной сети кафедры) с. 8-24	11	6
Проблема обеспечения кибербезопасности АСУ ТП	Основы кибербезопасности интеллектуальных энергосистем : Учебный курс для магистров / Семён Корт — Лаборатория Касперского, 2019 (в локальной сети кафедры) с. 45-59	11	6
Социальная инженерия	Основы кибербезопасности интеллектуальных энергосистем : Учебный курс для магистров / Семён Корт — Лаборатория Касперского, 2019 (в локальной сети кафедры) с. 106-113	11	6
Защита изолированных сетей	Основы кибербезопасности интеллектуальных энергосистем : Учебный курс для магистров / Семён Корт — Лаборатория Касперского, 2019 (в локальной сети кафедры) с. 95-105	11	6
Атаки на интеллектуальные АСУ ТП	Основы кибербезопасности интеллектуальных энергосистем : Учебный курс для магистров / Семён Корт — Лаборатория Касперского, 2019 (в локальной сети кафедры) с. 60-69	11	6
Введение	Основы кибербезопасности интеллектуальных энергосистем : Учебный курс для магистров / Семён Корт — Лаборатория Касперского, 2019 (в локальной сети кафедры) с. 3-7	11	5
Типовое вредоносное ПО АСУ ТП	Основы кибербезопасности интеллектуальных энергосистем : Учебный курс для магистров / Семён Корт — Лаборатория Касперского, 2019 (в локальной сети кафедры) с. 114-130	11	10,5
Организация подразделения обеспечения промышленной кибербезопасности. Политика безопасности	Основы кибербезопасности интеллектуальных энергосистем : Учебный курс для магистров / Семён	11	6

	Корт — Лаборатория Касперского, 2019 (в локальной сети кафедры) с. 131-134		
Функциональная безопасность АСУ ТП	Основы кибербезопасности интеллектуальных энергосистем : Учебный курс для магистров / Семён Корт — Лаборатория Касперского, 2019 (в локальной сети кафедры) с. 39-44	11	6
Безопасность сетей АСУ ТП	Основы кибербезопасности интеллектуальных энергосистем : Учебный курс для магистров / Семён Корт — Лаборатория Касперского, 2019 (в локальной сети кафедры) с. 70-94	11	16

6. Фонд оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации

Контроль качества освоения образовательной программы осуществляется в соответствии с Положением о балльно-рейтинговой системе оценивания результатов учебной деятельности обучающихся.

6.1. Контрольные мероприятия (КМ)

№ КМ	Се-местр	Вид контроля	Название контрольного мероприятия	Вес	Макс. балл	Порядок начисления баллов	Учи-тыва-ется в ПА
0	11	Проме-жуточная аттестация	экзамен	-	8	Защита отчета о выполнении задания осуществляется индивидуально. Студентом предоставляет выполненное задание. Оценивается качество правильность выводов и ответы на вопросы (задаются минимум 2 вопроса). При оценивании результатов используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179) Общий балл при оценке складывается из следующих показателей (за каждое задание): полностью выполнили базовую часть задания (1 балл), выполнили дополнительную часть задания (1 балл). Если студент в обозначенный срок не сдает работу минимум на базовую часть, то дополнительная часть становится обязательной и максимальный балл за задание становится (1 балл)	экзамен
1	11	Текущий контроль	Анализ протокола Modbus	1	3	Используя дамп трафика, определить: 1. Какие устройства ведомые, а какие ведущие (1 балл) 2. Найти взаимодействие, в котором осуществляется изменение регистров в ПЛК (1 балл) 3. Определить было ли вторжение в АСУ	экзамен

						ТП (1 балл)	

6.2. Процедура проведения, критерии оценивания

Не предусмотрены

6.3. Паспорт фонда оценочных средств

Компетенции	Результаты обучения	№ КМ	
		0	1
ПК-1	Знает: уязвимости современных АСУ ТП, подходы к устранению уязвимостей и построению системы защиты современных АСУ ТП	+	
ПК-1	Умеет: анализировать структуры АСУ ТП, строить их модели, оценивать риски функциональной безопасности, распознавать атаки социальной инженерии	+	
ПК-1	Имеет практический опыт: разработки политик безопасности современных промышленных систем автоматизации, исследования сетевых пакетов в промышленной сети	+	+
ПК-4	Знает: нормативные документы Российской федерации в области кибербезопасности; особенности организации подразделения центра управления инцидентами (ЦУИ ИБ) для поддержки информационной безопасности промышленной сети	+	
ПК-5	Знает: архитектуру автоматизированной системы управления технологическим процессом (АСУ ТП), модели промышленных систем автоматизации, сетевые технологии, используемые в современных АСУ ТП, понятия функциональной и информационной безопасности, их взаимосвязь и противоречия; основы организации своевременной и полноценной обработки инцидентов безопасности	+	
ПК-5	Умеет: работать со средствами обеспечения безопасности в системах промышленной автоматизации; настраивать межсетевой экран для обеспечения защиты периметра сети, для обеспечения сегментации внутренней сети	+	
ПК-5	Имеет практический опыт: анализа инцидентов кибербезопасности в современных промышленных системах автоматизации	+	+

Типовые контрольные задания по каждому мероприятию находятся в приложениях.

7. Учебно-методическое и информационное обеспечение дисциплины

Печатная учебно-методическая документация

а) основная литература:

Не предусмотрена

б) дополнительная литература:

Не предусмотрена

в) отечественные и зарубежные журналы по дисциплине, имеющиеся в библиотеке:

Не предусмотрены

г) методические указания для студентов по освоению дисциплины:

1. Баринов А.Е. Методические указания по дисциплине "Кибербезопасность интеллектуальных автоматизированных систем управления технологическими процессами"

из них: учебно-методическое обеспечение самостоятельной работы студента:

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
1	Основная литература	Электронно-библиотечная система издательства Лань	Сергеев, А. Н. Основы локальных компьютерных сетей : учебное пособие для вузов / А. Н. Сергеев. — 3-е изд., стер. — Санкт-Петербург : Лань, 2021. — 184 с. — ISBN 978-5-8114-6855-3. https://e.lanbook.com/book/152651
2	Дополнительная литература	Электронно-библиотечная система издательства Лань	Интегрированные системы проектирования и управления. SCADA : учебное пособие / Х. Н. Музипов, О. Н. Кузяков, С. А. Хохрин [и др.]. — Санкт-Петербург : Лань, 2021. — 408 с. — ISBN 978-5-8114-3265-3. https://e.lanbook.com/book/169310
3	Дополнительная литература	Электронно-библиотечная система издательства Лань	Дадаян, Л. Г. Автоматизированные системы управления технологическими процессами : учебное пособие / Л. Г. Дадаян. — Уфа : УГНТУ, 2018. — 241 с. — ISBN 978-5-7831-1676-6. https://e.lanbook.com/book/166886

Перечень используемого программного обеспечения:

Нет

Перечень используемых профессиональных баз данных и информационных справочных систем:

Нет

8. Материально-техническое обеспечение дисциплины

Не предусмотрено