ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Руководитель специальности

ЮУрГУ
Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Соколов А. Н.
Пользователь: sokolovan
Дата подписания: 02.07.2024

А. Н. Соколов

РАБОЧАЯ ПРОГРАММА

дисциплины 1.Ф.02 Современные киберугрозы в промышленных и корпоративных системах автоматизации
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.

ЮУрГУ
Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Соколов А. Н.
Пользователь: sokolovan
Дата подписания: 02.07.2024

А. Н. Соколов

Разработчик программы,
к.физ.-мат.н., доц., доцент

ЮУрГУ
Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Ручай А. Н.
Пользователь: ruchaian
Дата подписания: 01.07.2024

А. Н. Ручай

Челябинск

1. Цели и задачи дисциплины

Изучение основ киберугроз в промышленных и корпоративных системах автоматизации. Изучение методов и подходов к оценке киберугроз в промышленных и корпоративных системах автоматизации

Краткое содержание дисциплины

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. Идентификация и моделирование каналов возможного деструктивного информационно-технического воздействия в промышленных и корпоративных системах автоматизации. Анализ и оценка рисков информационной безопасности в промышленных и корпоративных системах автоматизации. Анализ современных киберугроз в промышленных и корпоративных системах автоматизации, актуальные векторы атак на промышленные сети АСУ ТП. Оценка уязвимостей по отношению к современным киберугрозам промышленных сетей АСУ ТП.

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: актуальные угрозы информационной безопасности промышленных компаний, текущее состояние и эволюцию киберугроз как ответную реакцию на внедрение средств и мер информационной безопасности Умеет: анализировать и оценивать риски информационной безопасности в промышленных и корпоративных системах автоматизации Имеет практический опыт: идентификации и моделирования каналов возможного деструктивного информационно-технического воздействия в промышленных и корпоративных системах автоматизации
ПК-3 Способен выполнять работы по мониторингу и аудиту защищенности информации в автоматизированных системах	Знает: 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: проводить аналитику современных киберугроз в промышленных и корпоративных системах автоматизации, актуальные векторы атак на промышленные сети АСУ ТП Имеет практический опыт: оценки уязвимостей

	по отношению к современным киберугрозам промышленных сетей АСУ ТП

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Нет	1.Ф.06 Мониторинг информационной безопасности автоматизированных систем управления, 1.Ф.07 Защита электронного документооборота, 1.Ф.05 Кодирование информации в автоматизированных системах управления, 1.Ф.09 Кибербезопасность интеллектуальных автоматизированных систем управления технологическими процессами, 1.Ф.10 Математическое моделирование информационных потоков и систем защиты информации

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

Нет

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 3 з.е., 108 ч., 54,25 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		9
Общая трудоёмкость дисциплины	108	108
Аудиторные занятия:	48	48
Лекции (Л)	32	32
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	16	16
Лабораторные работы (ЛР)	0	0
Самостоятельная работа (СРС)	53,75	53,75
Руководство	28,75	28.75
База знаний	25	25
Консультации и промежуточная аттестация	6,25	6,25
Вид контроля (зачет, диф.зачет, экзамен)	-	зачет

5. Содержание дисциплины

№	Наименование разделов дисциплины	Объем аудиторных занятий

раздела		по видам в часах			
		Всего	Л	ПЗ	ЛР
1	Основные понятия и определения. Киберугрозы в промышленных и корпоративных системах автоматизации	24	16	8	0
2	Оценка киберугроз в промышленных и корпоративных системах автоматизации	24	16	8	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Актуальные угрозы информационной безопасности промышленных компаний, текущее состояние и эволюцию киберугроз как ответную реакцию на внедрение средств и мер информационной безопасности	6
2	1	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	6
5	1	Идентификация и моделирование каналов возможного деструктивного информационно-технического воздействия в промышленных и корпоративных системах автоматизации	4
3	2	Анализ и оценка рисков информационной безопасности в промышленных и корпоративных системах автоматизации	4
4	2	Анализ современных киберугроз в промышленных и корпоративных системах автоматизации, актуальные векторы атак на промышленные сети АСУ ТП	6
6	2	Оценка уязвимостей по отношению к современным киберугрозам промышленных сетей АСУ ТП	6

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	1	Идентификация каналов возможного деструктивного информационно-технического воздействия в промышленных и корпоративных системах автоматизации	4
2	1	Моделирование каналов возможного деструктивного информационно-технического воздействия в промышленных и корпоративных системах автоматизации	4
3	2	Оценка уязвимостей по отношению к современным киберугрозам промышленных сетей АСУ ТП	4
4	2	Анализ современных киберугроз в промышленных и корпоративных системах автоматизации,	4

5.3. Лабораторные работы

Не предусмотрены

5.4. Самостоятельная работа студента

Выполнение СРС

Подвид СРС	Список литературы (с указанием разделов, глав, страниц) / ссылка на ресурс	Семестр	Кол-во часов
Руководство	Руководство ATT&CK ICS для характеристики и описания киберугроз в промышленных и корпоративных системах автоматизации	9	28,75
База знаний	База знаний ATT&CK ICS для характеристики и описания поведения злоумышленника после компрометации https://collaborate.mitre.org/attackics/index.php/All_Techniques	9	25

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
1	9	Текущий контроль	Идентификация и моделирование каналов возможного деструктивного информационно-технического воздействия в промышленных и корпоративных системах автоматизации	1	40	При оценивании результатов учебной деятельности обучающегося по дисциплине используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Показатели оценивания. При условии корректного и полного заполнения задания обучающему начисляется 40 баллов. Максимальное количество баллов - 40. Весовой коэффициент - 1.	зачет
2	9	Текущий контроль	Анализ современных киберугроз в промышленных и корпоративных системах автоматизации, актуальные векторы атак на промышленные сети АСУ ТП	1	40	При оценивании результатов учебной деятельности обучающегося по дисциплине используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). При условии корректного и полного заполнения задания обучающему начисляется 40 баллов. Максимальное количество баллов - 40. Весовой коэффициент - 1.	зачет
3	9	Проме-жуточная аттестация	Зачет	-	40	При оценивании результатов учебной деятельности обучающегося по дисциплине используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом	зачет

						ректора от 24.05.2019 г. № 179). Показатели оценивания. 50 баллов – ответ на вопрос содержит логичное, последовательное изложение материала с соответствующими выводами и обоснованными положениями; 30 баллов – ответ содержит в целом грамотно изложенную теоретическую главу, однако с не вполне обоснованными выводами; 10 балл – ответ базируется на практическом материале, но имеет поверхностный анализ, просматривается непоследовательность изложения материала, представлены необоснованные выводы; 0 баллов - ответ отсутствует.	

6.2. Процедура проведения, критерии оценивания

Вид промежуточной аттестации	Процедура проведения	Критерии оценивания
зачет	Зачтено: Рейтинг обучающегося за мероприятие больше или равен 60 %. Не зачтено: Рейтинг обучающегося за мероприятие меньше 60 %	В соответствии с пп. 2.5, 2.6 Положения

6.3. Паспорт фонда оценочных средств

Компетенции	Результаты обучения	№ КМ		
		1	2	3
ПК-1	Знает: актуальные угрозы информационной безопасности промышленных компаний, текущее состояние и эволюцию киберугроз как ответную реакцию на внедрение средств и мер информационной безопасности	+		+
ПК-1	Умеет: анализировать и оценивать риски информационной безопасности в промышленных и корпоративных системах автоматизации	+		+
ПК-1	Имеет практический опыт: идентификации и моделирования каналов возможного деструктивного информационно-технического воздействия в промышленных и корпоративных системах автоматизации	+		+
ПК-3	Знает: 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		+	+
ПК-3	Умеет: проводить аналитику современных киберугроз в промышленных и корпоративных системах автоматизации, актуальные векторы атак на промышленные сети АСУ ТП		+	+
ПК-3	Имеет практический опыт: оценки уязвимостей по отношению к современным киберугрозам промышленных сетей АСУ ТП		+	+

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. Руководство ATT&CK ICS для характеристики и описания киберугроз в промышленных и корпоративных системах автоматизации

из них: учебно-методическое обеспечение самостоятельной работы студента:

1. Руководство ATT&CK ICS для характеристики и описания киберугроз в промышленных и корпоративных системах автоматизации

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
1	Основная литература	Электронно-библиотечная система издательства Лань	Диогенес, Ю. Кибербезопасность. стратегия атак и обороны / Ю. Диогенес, Э. Озкайя ; перевод с английского Д. А. Беликова. — Москва : ДМК Пресс, 2020. — 326 с. — ISBN 978-5-97060-709-1. — Текст : электронный // Лань : электронно-библиотечная система. https://e.lanbook.com/book/131717
2	Дополнительная литература	Электронно-библиотечная система издательства Лань	Белоус, А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами / А. И. Белоус, В. А. Солодуха. — Вологда : Инфра-Инженерия, 2020. — 692 с. — ISBN 978-5-9729-0486-0. — Текст : электронный // Лань : электронно-библиотечная система. https://e.lanbook.com/book/148383
3	Основная литература	Электронно-библиотечная система издательства Лань	Белоус, А. И. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения : энциклопедия / А. И. Белоус, В. А. Солодуха. — Москва : Техносфера, 2021. — 482 с. — ISBN 978-5-94836-612-8. — Текст : электронный // Лань : электронно-библиотечная система. https://e.lanbook.com/book/181222
4	Основная литература	Электронно-библиотечная система издательства Лань	Белоус, А. И. Кибербезопасность объектов топливно-энергетического комплекса. Концепции, методы и средства обеспечения / А. И. Белоус. — Вологда : Инфра-Инженерия, 2020. — 644 с. — ISBN 978-5-9729-0512-6. — Текст : электронный // Лань : электронно-библиотечная система. https://e.lanbook.com/book/148386
5	Дополнительная литература	Электронно-библиотечная система Znanium.com	Бабаш, А. В. Моделирование системы защиты информации. Практикум : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 3-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 320 с. https://znanium.com/catalog/product/1232287

Перечень используемого программного обеспечения:

1. Microsoft-Windows(бессрочно)
2. Microsoft-Office(бессрочно)
3. Python Software Foundation-Python (бессрочно)
4. -Python(бессрочно)

Перечень используемых профессиональных баз данных и информационных справочных систем:

1. ООО "ГарантУралСервис"-Гарант(31.12.2022)

8. Материально-техническое обеспечение дисциплины

Не предусмотрено