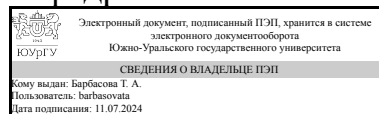


ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Заведующий выпускающей
кафедрой



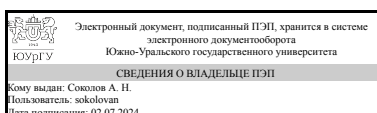
Т. А. Барбасова

РАБОЧАЯ ПРОГРАММА

дисциплины 1.Ф.М0.06.01 Кибербезопасность в интернете вещей
для направления 27.04.04 Управление в технических системах
уровень Магистратура
магистерская программа Программно-технические средства и системы автоматизации управления
форма обучения очная
кафедра-разработчик Защита информации

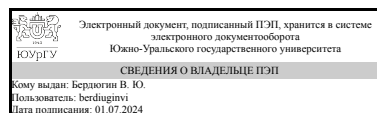
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 27.04.04 Управление в технических системах, утверждённым приказом Минобрнауки от 11.08.2020 № 942

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



А. Н. Соколов

Разработчик программы,
доцент



В. Ю. Бердюгин

1. Цели и задачи дисциплины

Целями освоения дисциплины «Кибербезопасность в Интернете вещей» являются изучение: - основных понятий в области обеспечения информационной безопасности; - требований нормативно-правовых документов по защите объектов критической информационной инфраструктуры; - ответственности за нарушение требований нормативно-правовых документов по защите объектов критической информационной инфраструктуры; - основных угроз, уязвимостей, рисков в области безопасности Интернета вещей, киберфизических систем в составе объектов критической информационной инфраструктуры; - технологий угроз сетевой безопасности, а также механизмов противодействия сетевым атакам; - особенностей проектирования систем безопасности объектов критической информационной инфраструктуры.

Краткое содержание дисциплины

В рамках данной дисциплины обучающиеся изучают: основные нормативно-правовые акты РФ, международные и национальные стандарты в области обеспечения безопасности Интернета вещей, киберфизических систем, объектов критической информационной инфраструктуры; протоколы обеспечения безопасности на сетевом уровне, применяемые в Интернете вещей; особенности обеспечения безопасности промышленного Интернета вещей; применение требований нормативных, руководящих и методических документов РФ, а также национальных стандартов и лучших практик в области информационной безопасности для обеспечения безопасности киберфизических систем, объектов критической информационной инфраструктуры.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине
ПК-3 Способен управлять защитой информации в автоматизированных системах	Знает: методы защиты информации в автоматизированных системах, построенных на основе применения технологий интернета вещей Умеет: управлять защитой информации в автоматизированных системах, построенных на основе применения технологий интернета вещей Имеет практический опыт: управления защитой информации в автоматизированных системах, построенных на основе применения технологий интернета вещей

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Нет	Не предусмотрены

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
		3
Общая трудоёмкость дисциплины	108	108
<i>Аудиторные занятия:</i>	48	48
Лекции (Л)	32	32
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	16	16
Лабораторные работы (ЛР)	0	0
<i>Самостоятельная работа (СРС)</i>	53,75	53,75
Подготовка тематических докладов и рефератов по вопросам, выносимым на практические занятия (разделы 3-4).	16	16
Подготовка тематических докладов и рефератов по вопросам, выносимым на практические занятия (разделы 5-6).	21,75	21.75
Подготовка тематических докладов и рефератов по вопросам, выносимым на практические занятия (разделы 1-2).	16	16
Консультации и промежуточная аттестация	6,25	6,25
Вид контроля (зачет, диф.зачет, экзамен)	-	зачет

5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах			
		Всего	Л	ПЗ	ЛР
1	Основные понятия в области обеспечения информационной безопасности.	6	4	2	0
2	Понятие Интернета вещей. Промышленный и бытовой Интернет вещей. Критическая информационная инфраструктура Российской Федерации.	6	4	2	0
3	Ответственность за нарушение требований нормативно-правовых документов по защите объектов критической информационной инфраструктуры.	6	4	2	0
4	Основные угрозы, уязвимости и риски в области безопасности Интернета вещей, киберфизических систем в составе объектов критической информационной инфраструктуры.	12	8	4	0
5	Технологии угроз сетевой безопасности, механизмы противодействия сетевым атакам.	6	4	2	0

6	Особенности проектирования систем безопасности объектов критической информационной инфраструктуры.	12	8	4	0
---	--	----	---	---	---

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Понятие национальной безопасности Российской Федерации. Роль и место информационной безопасности в системе национальной безопасности.	2
2	1	Национальные интересы Российской Федерации в информационной сфере. Виды и источники угроз информационной безопасности.	2
3	2	Понятие Интернета вещей. Промышленный и бытовой Интернет вещей.	2
4	2	Понятие критической информационной инфраструктуры Российской Федерации. Критерии и процедура категорирования объектов критической информационной инфраструктуры.	2
5	3	Обязанности субъектов критической информационной инфраструктуры. Организация контроля за соблюдением требований нормативно-правовых документов по защите объектов критической информационной инфраструктуры.	2
6	3	Уголовная и административная ответственность за нарушение требований нормативно-правовых документов по защите объектов критической информационной инфраструктуры.	2
7-8	4	Основные угрозы, уязвимости и риски в области безопасности Интернета вещей, киберфизических систем в составе объектов критической информационной инфраструктуры.	4
9-10	4	Основные этапы обеспечения безопасности, построение модели угроз безопасности Интернета вещей, киберфизических систем в составе объектов критической информационной инфраструктуры.	4
11	5	Основные нормативно-правовые акты РФ в области обеспечения безопасности Интернета вещей, киберфизических систем, объектов критической информационной инфраструктуры	2
12	5	Международные и национальные стандарты в области обеспечения безопасности Интернета вещей, киберфизических систем, объектов критической информационной инфраструктуры	2
13=14	6	Система мер по обеспечению безопасности значимых объектов критической информационной инфраструктуры. Протоколы обеспечения безопасности на сетевом уровне, применяемые в Интернете вещей.	4
15-16	6	Государственная система обнаружения, предотвращения и ликвидации компьютерных атак. Моделирование системы противодействия компьютерным атакам на объекты критической информационной инфраструктуры.	4

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	1	Понятие национальной безопасности Российской Федерации. Национальные интересы и угрозы национальной безопасности в информационной сфере. Источники угроз информационной безопасности.	2
2	2	Понятие Интернета вещей. Промышленный и бытовой Интернет вещей. Критическая информационная инфраструктура Российской Федерации.	2

3	3	Уголовная и административная ответственность за нарушение требований нормативно-правовых документов по защите объектов критической информационной инфраструктуры.	2
4	4	Основные угрозы, уязвимости и риски в области безопасности Интернета вещей, киберфизических систем в составе объектов критической информационной инфраструктуры.	2
5	4	Основные этапы обеспечения безопасности, построение модели угроз безопасности Интернета вещей, киберфизических систем в составе объектов критической информационной инфраструктуры.	2
6	5	Основные нормативно-правовые акты РФ в области обеспечения безопасности Интернета вещей, киберфизических систем, объектов критической информационной инфраструктуры	2
7	6	Протоколы обеспечения безопасности на сетевом уровне, применяемые в Интернете вещей, особенности обеспечения безопасности промышленного Интернета вещей.	2
8	6	Моделирование системы противодействия компьютерным атакам на объекты критической информационной инфраструктуры (деловая игра).	2

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
Подготовка тематических докладов и рефератов по вопросам, выносимым на практические занятия (разделы 3-4).	1. Белоус, А. И. Кибербезопасность объектов топливно-энергетического комплекса. Концепции, методы и средства обеспечения / А. И. Белоус. — Вологда : Инфра-Инженерия, 2020. Глава 2. Кибероружие - классификация средств и методов применения. 2. Криулин, А. А. Основы безопасности прикладных информационных технологий и систем : учебное пособие / А. А. Криулин, В. С. Нефедов, С. И. Смирнов. — Москва : РТУ МИРЭА, 2020, Глава 3. Политика информационной безопасности. 3. Лекции преподавателя. Теория информационной безопасности и методология защиты информации, конспект (стр. 65 - 72)	3	16
Подготовка тематических докладов и рефератов по вопросам, выносимым на практические занятия (разделы 5-6).	1. Криулин, А. А. Основы безопасности прикладных информационных технологий и систем : учебное пособие / А. А. Криулин, В. С. Нефедов, С. И. Смирнов. — Москва : РТУ МИРЭА, 2020, Глава 5. Основы поиска уязвимостей программного обеспечения. 2. Белоус, А. И. Кибербезопасность объектов топливно-энергетического комплекса.	3	21,75

	Концепции, методы и средства обеспечения / А. И. Белоус. — Вологда : Инфра-Инженерия, 2020. Глава 3. Кибербезопасность электроэнергетических инфраструктур. 3. Кибербезопасность. стратегия атак и обороны / Ю. Диогенес, Э. Озкая ; перевод с английского Д. А. Беликова. — Москва : ДМК Пресс, 2020. Глава 2. Процесс реагирования на компьютерные инциденты. 4. Лекции преподавателя. Теория информационной безопасности и методология защиты информации, конспект (стр. 80 - 87, 96 - 103)		
Подготовка тематических докладов и рефератов по вопросам, выносимым на практические занятия (разделы 1-2).	1. Криулин, А. А. Основы безопасности прикладных информационных технологий и систем : учебное пособие / А. А. Криулин, В. С. Нефедов, С. И. Смирнов. — Москва : РТУ МИРЭА, 2020, Глава 1. Теоретические основы информационной безопасности. 2. Лекции преподавателя. Теория информационной безопасности и методология защиты информации, конспект (стр. 1- 25, 59-65)	3	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	Учитывается в ПА
1	3	Текущий контроль	Выступление с докладом на практическом занятии (разделы 1-2)	1	6	За неделю до семинарского занятия группе задается перечень тем (8-10) для выступления. Время, отведенное на каждое выступление, 10-15 минут. Тезисы доклада и презентация представляются в виде отчета в электронный ЮУрГУ. При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Показатели оценивания: 1. Соответствие заданию, знание нормативно-правовой базы: 2 балла —	зачет

						полное соответствие заданию, все ссылки на нормативно-правовые документы корректны; 2 балл – в целом соответствие заданию, однако имеются ссылки на утратившие актуальность нормативно-правовые документы; 0 баллов – не соответствие заданию; 2. Качество оформления практической работы и презентации: 2 балла – работа имеет логичное, последовательное изложение материала. презентация дополняет и иллюстрирует доклад; 1 балл – работа в целом имеет, последовательное изложение материала, однако презентация содержит только тезисы доклада; 0 баллов - просматривается непоследовательность изложения материала, презентация не соответствует содержанию доклада. 3. Качество выступления: 2 балла – студент демонстрирует глубокое знание вопросов темы, грамотно формулирует выводы и предложения, уверенно отвечает на уточняющие вопросы; 1 балл – в процессе выступления студент в целом показывает знание вопросов темы, однако затрудняется при формулировании выводов и предложений, неуверенно отвечает на уточняющие вопросы; 0 баллов – студент проявляет неуверенность, демонстрирует слабое знание вопросов темы, не в состоянии сформулировать выводы и предложения.	
2	3	Текущий контроль	Тестирование (разделы 1-2)	1	10	По окончании изучения раздела2 дисциплины проводится тестирование, в процессе которого студентам предлагается выбрать правильный ответ на вопросы из предложенного перечня. При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Всего необходимо ответить на 10 вопросов. Каждый правильный ответ - 1 балл. Максимальное количество баллов – 10.	зачет
3	3	Текущий контроль	Выступление с докладом на практическом занятии (разделы 3-4)	1	6	За неделю до семинарского занятия группе задается перечень тем (8-10) для выступления. Время, отведенное на каждое выступление, 10-15 минут. Тезисы доклада и презентация представляются в виде отчета в электронный ЮУрГУ. При оценивании	зачет

					результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Показатели оценивания: 1. Соответствие заданию, знание нормативно-правовой базы: 2 балла – полное соответствие заданию, все ссылки на нормативно-правовые документы корректны; 2 балл – в целом соответствие заданию, однако имеются ссылки на утратившие актуальность нормативно-правовые документы; 0 баллов – не соответствие заданию; 2. Качество оформления практической работы и презентации: 2 балла – работа имеет логичное, последовательное изложение материала. презентация дополняет и иллюстрирует доклад; 1 балл – работа в целом имеет, последовательное изложение материала, однако презентация содержит только тезисы доклада; 0 баллов - просматривается непоследовательность изложения материала, презентация не соответствует содержанию доклада. 3. Качество выступления: 2 балла – студент демонстрирует глубокое знание вопросов темы, грамотно формулирует выводы и предложения, уверенно отвечает на уточняющие вопросы; 1 балл – в процессе выступления студент в целом показывает знание вопросов темы, однако затрудняется при формулировании выводов и предложений, неуверенно отвечает на уточняющие вопросы; 0 баллов – студент проявляет неуверенность, демонстрирует слабое знание вопросов темы, не в состоянии сформулировать выводы и предложения.		
4	3	Текущий контроль	Тестирование (разделы 3-4)	1	10	По окончании изучения раздела 4 дисциплины проводится тестирование, в процессе которого студентам предлагается выбрать правильный ответ на вопросы из предложенного перечня. При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Всего необходимо ответить на 10 вопросов. Каждый правильный ответ - 1 балл. Максимальное количество баллов –	зачет

					10.		
5	3	Текущий контроль	Выступление с докладом на практическом занятии (разделы 5-6)	1	6	За неделю до семинарского занятия группе задается перечень тем (8-10) для выступления. Время, отведенное на каждое выступление, 10-15 минут. Тезисы доклада и презентация представляются в виде отчета в электронный ЮУрГУ. При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Показатели оценивания: 1. Соответствие заданию, знание нормативно-правовой базы: 2 балла – полное соответствие заданию, все ссылки на нормативно-правовые документы корректны; 2 балл – в целом соответствие заданию, однако имеются ссылки на утратившие актуальность нормативно-правовые документы; 0 баллов – не соответствие заданию; 2. Качество оформления практической работы и презентации: 2 балла – работа имеет логичное, последовательное изложение материала. презентация дополняет и иллюстрирует доклад; 1 балл – работа в целом имеет, последовательное изложение материала, однако презентация содержит только тезисы доклада; 0 баллов - просматривается непоследовательность изложения материала, презентация не соответствует содержанию доклада. 3. Качество выступления: 2 балла – студент демонстрирует глубокое знание вопросов темы, грамотно формулирует выводы и предложения, уверенно отвечает на уточняющие вопросы; 1 балл – в процессе выступления студент в целом показывает знание вопросов темы, однако затрудняется при формулировании выводов и предложений, неуверенно отвечает на уточняющие вопросы; 0 баллов – студент проявляет неуверенность, демонстрирует слабое знание вопросов темы, не в состоянии сформулировать выводы и предложения.	зачет
6	3	Бонус	Посещаемость	-	3	При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). В случае	зачет

						отсутствия пропусков занятий без уважительной причины студенту прибавляется 3 бонусных балла.	
7	3	Промежуточная аттестация	Зачет	-	10	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). По результатам выполненных мероприятий текущего контроля в процентном выражении формируется оценка за курс. При условии выполнения мероприятий текущего контроля и достижении 60 - 100 % рейтинга обучающийся получает зачет. Если рейтинг составляет менее 60%, обучающийся сдает зачет по билету, который включает 2 теоретических вопроса по пройденным разделам, преподаватель проверяет, беседует и оценивает. Показатели оценивания ответов по каждому из вопросов: 5 баллов – студент обладает твёрдым и полным знанием материала дисциплины, уверенно отвечает на дополнительные вопросы, логически, грамотно и точно излагает материал дисциплины, интерпретируя его самостоятельно, способен самостоятельно его анализировать и делать выводы; 4 балла – студент знает материал дисциплины в запланированном объёме, некоторые моменты в ответе не отражены или допускает несущественные неточности; грамотно и по существу излагает материал. 3 балла – студент знает только основной материал дисциплины, не усвоил его деталей, допускает неточности в изложении и интерпретации знаний; имеются нарушения логической последовательности 2 балла – студент не знает значительной части материала дисциплины; допускает грубые ошибки при ответе на дополнительные вопросы. Максимальное число баллов - 10. Студент получает зачет, если суммарная оценка составляет не менее 6 баллов.	зачет

6.2. Процедура проведения, критерии оценивания

Вид промежуточной аттестации	Процедура проведения	Критерии оценивания
------------------------------	----------------------	---------------------

зачет	В процессе проведения зачета студенты в аудитории письменно отвечают на вопросы билета, который включает 2 теоретических вопроса по пройденным разделам, преподаватель проверяет, беседует и оценивает. Зачет также может проводиться в дистанционном формате в режиме видеоконференции в "Электронном ЮУрГУ" в соответствии с регламентом, утвержденном приказом ректора ЮУрГУ от 21.04.2020 № 80.	В соответствии с пп. 2.5, 2.6 Положения
-------	---	---

6.3. Паспорт фонда оценочных средств

Компетенции	Результаты обучения	№ КМ						
		1	2	3	4	5	6	7
ПК-3	Знает: методы защиты информации в автоматизированных системах, построенных на основе применения технологий интернета вещей	+	+	+	+	+	+	+
ПК-3	Умеет: управлять защитой информации в автоматизированных системах, построенных на основе применения технологий интернета вещей	+	+	+	+	+	+	+
ПК-3	Имеет практический опыт: управления защитой информации в автоматизированных системах, построенных на основе применения технологий интернета вещей	+	+	+	+	+	+	+

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. Лекции преподавателя

из них: учебно-методическое обеспечение самостоятельной работы студента:

1. Лекции преподавателя

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
1	Основная литература	Электронно-библиотечная система издательства Лань	Криулин, А. А. Основы безопасности прикладных информационных технологий и систем : учебное пособие / А. А. Криулин, В. С. Нефедов, С. И. Смирнов. — Москва : РТУ МИРЭА, 2020. — 136 с. — Текст : электронный // Лань : электроннобиблиотечная система. — URL:

			https://e.lanbook.com/book/167606
2	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
3	Дополнительная литература	Электронно-библиотечная система издательства Лань	Диогенес, Ю. Кибербезопасность. стратегия атак и обороны / Ю. Диогенес, Э. Озкая ; 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

Перечень используемого программного обеспечения:

Нет

Перечень используемых профессиональных баз данных и информационных справочных систем:

1. -База данных polpred (обзор СМИ)(бессрочно)
2. ООО "ИВИС"-База данных периодических изданий "ИВИС"(18.03.2024)

8. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Практические занятия и семинары	906 (36)	Комплект компьютерного оборудования, минитор, маршрутизатор, программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozilla Firefox, Консультант+; Операционные системы семейства Linux, Windows, СУБД промышленного масштаба (например, Microsoft SQL Server 2010, Oracle 9i и т.п), свободно распространяемые пакеты прикладных программ: утилиты резервного копирования и восстановления файловых систем и разделов НЖМД; средства диагностики и тестирования ПК; межсетевые экраны; системы обнаружения вторжений; антивирусы.
Лекции	906 (36)	Комплект компьютерного оборудования, LCD Проектор, Экран проекционный, настенные стенды по защите информации (5 шт.), программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozilla Firefox, Консультант+.