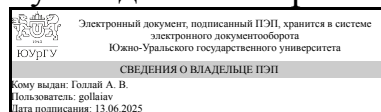


ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Руководитель направления



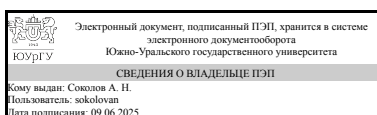
А. В. Голлай

РАБОЧАЯ ПРОГРАММА

дисциплины 1.О.02 Кибербезопасность
для направления 09.04.02 Информационные системы и технологии
уровень Магистратура
форма обучения очная
кафедра-разработчик Защита информации

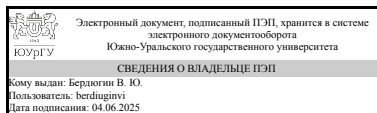
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 09.04.02 Информационные системы и технологии, утверждённым приказом Минобрнауки от 19.09.2017 № 917

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 индустриального 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
ОПК-5 Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем	Знает: основные понятия, источники и угрозы кибербезопасности информационных и автоматизированных систем; средства и способы обеспечения кибербезопасности; принципы построения систем защиты информации Умеет: классифицировать и оценивать угрозы кибербезопасности информационных и автоматизированных систем Имеет практический опыт: принимать решения по обеспечению кибербезопасности информационных и автоматизированных систем

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., 42,25 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		4
Общая трудоёмкость дисциплины	108	108
<i>Аудиторные занятия:</i>	36	36
Лекции (Л)	24	24
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	12	12
Лабораторные работы (ЛР)	0	0
<i>Самостоятельная работа (СРС)</i>	65,75	65,75
Подготовка тематических докладов и рефератов по вопросам, выносимым на практические занятия (разделы 1-2).	20	20
Подготовка тематических докладов и рефератов по вопросам, выносимым на практические занятия (разделы 3-4).	20	20
Подготовка тематических докладов и рефератов по вопросам, выносимым на практические занятия (разделы 5-6).	25,75	25.75
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.	4	2	2	0
2	Требования нормативно-правовых документов по защите объектов критической информационной инфраструктуры.	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.	8	6	2	0
5	Технологии угроз сетевой безопасности, механизмы противодействия сетевым атакам.	6	4	2	0
6	Особенности проектирования систем безопасности объектов	6	4	2	0

	критической информационной инфраструктуры.				
--	--	--	--	--	--

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Основные понятия в области обеспечения информационной безопасности.	2
2	2	Требования нормативно-правовых документов по защите объектов критической информационной инфраструктуры.	4
3	3	Ответственность за нарушение требований нормативно-правовых документов по защите объектов критической информационной инфраструктуры.	4
4	4	Виды угроз безопасности Интернета вещей, киберфизических систем в составе объектов критической информационной инфраструктуры.	2
5	4	Моделирование угроз безопасности Интернета вещей, киберфизических систем в составе объектов критической информационной инфраструктуры.	4
6	5	Технологии угроз сетевой безопасности, механизмы противодействия сетевым атакам.	4
7	6	Основные требования к системам безопасности объектов критической информационной инфраструктуры.	2
8	6	Особенности проектирования систем безопасности объектов критической информационной инфраструктуры.	2

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.. Роль и место информационной безопасности в системе национальной безопасности. Виды и источники угроз информационной безопасности.	2
2	2	Понятие критической информационной инфраструктуры Российской Федерации. Обязанности субъектов критической информационной инфраструктуры. Критерии и процедура категорирования объектов критической информационной инфраструктуры.	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	5	Основные нормативно-правовые акты РФ в области обеспечения безопасности Интернета вещей, киберфизических систем, объектов критической информационной инфраструктуры	2
6	6	Система мер по обеспечению безопасности значимых объектов критической информационной инфраструктуры.	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 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)	4	20
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)	4	20
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. 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. Озкайя ; перевод с английского Д. А. Беликова. — Москва : ДМК Пресс, 2020. Глава 2. Процесс реагирования на компьютерные инциденты. 4. Лекции преподавателя. Теория информационной безопасности и	4	25,75

	методология защиты информации, конспект (стр. 80 - 87, 96 - 103)		
--	---	--	--

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	4	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 – 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	зачет

						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	4	Текущий контроль	Тестирование (разделы 1-2)	1	10	По окончании изучения раздела 2 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	4	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 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	зачет

						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	4	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 – 10.	зачет
5	4	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;	зачет

						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.	
6	4	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 отсутствия пропусков занятий без уважительной причины студенту прибавляется 3 бонусных балла.	зачет
7	4	Промежуточная аттестация	Зачет	-	10	При оценивании результатов учебной деятельности студента по дисциплине используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). 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. Показатели оценивания ответов по каждому из вопросов: 5 баллов – студент обладает твердым и полным знанием материала дисциплины, уверенно отвечает на дополнительные вопросы, логически, грамотно и точно излагает материал дисциплины, интерпретируя его самостоятельно, способен	зачет

					самостоятельно его анализировать и делать выводы; 4 балла – студент знает материал дисциплины в запланированном объеме, 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.	
--	--	--	--	--	--	--

6.2. Процедура проведения, критерии оценивания

Вид промежуточной аттестации	Процедура проведения	Критерии оценивания
зачет	При оценивании результатов учебной деятельности студента по дисциплине используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). 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. Показатели оценивания ответов по каждому из вопросов: 5 баллов – студент обладает твердым 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 объеме, 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.	В соответствии с пп. 2.5, 2.6 Положения

6.3. Паспорт фонда оценочных средств

Компетенции	Результаты обучения	№ KM						
		1	2	3	4	5	6	7
ОПК-5	Знает: основные понятия, источники и угрозы кибербезопасности информационных и автоматизированных систем; средства и способы обеспечения кибербезопасности; принципы построения систем защиты	+	+	+	+	+	+	+

Нет

Перечень используемых профессиональных баз данных и информационных справочных систем:

Нет

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+.