

ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Директор института
Высшая школа электроники и
компьютерных наук

ЮУрГУ
Южно-Уральский государственный университет
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Голлай А. В.
Пользователь: gollaiav
Дата подписания: 21.06.2024

А. В. Голлай

РАБОЧАЯ ПРОГРАММА

дисциплины В.1.10 Методы и средства противодействия террористической деятельности в системах управления критически важных объектов
для специальности 10.05.03 Информационная безопасность автоматизированных систем

уровень специалист **тип программы** Специалитет

специализация Информационная безопасность автоматизированных систем критически важных объектов

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 01.12.2016 № 1509

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

ЮУрГУ
Южно-Уральский государственный университет
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Соколов А. Н.
Пользователь: sokolovan
Дата подписания: 21.06.2024

А. Н. Соколов

Разработчик программы,
доцент

ЮУрГУ
Южно-Уральский государственный университет
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Бердюгин В. Ю.
Пользователь: berduginvi
Дата подписания: 18.06.2024

В. Ю. Бердюгин

1. Цели и задачи дисциплины

Целью преподавания дисциплины является знакомство студентов с современным состоянием и тенденциями преступности террористического характера, системой борьбы с терроризмом в России и за рубежом, а также обучение мерам противодействия террористической деятельности в системах управления критически важных объектов. Задачами дисциплины являются: - изучение технологий, средств и систем обеспечения информационной безопасности критически важных объектов и систем управления ими; - выработка умений и навыков определять комплекс мер противодействия террористической деятельности в системах управления критически важных объектов; - изучение подходов к созданию, эксплуатации и развитию систем обеспечения информационной безопасности критически важных объектов; - выработка навыков анализа угроз безопасности и уязвимостей систем управления критически важных объектов; - обучение принципам выбора и применения средств анализа защищенности, активного аудита и обнаружения вторжений, а также средств аудита исходного кода программ на предмет обнаружения потенциальных уязвимостей.

Краткое содержание дисциплины

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине (ЗУны)
ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	Знать:нормативно-методические и руководящие документы, регламентирующие обеспечение информационной безопасности критически важных объектов, способы выявления угроз информационной безопасности на критически важных объектах Уметь:формулировать основные требования к методам и средствам защиты информации на критически важных объектах Владеть:навыками анализа угроз и уязвимости информационной безопасности для критически важных объектов и автоматизированных систем критически важных объектов
ОПК-6 способностью применять нормативные правовые акты в профессиональной деятельности	Знать:основные нормативно-правовые акты, регламентирующие обеспечение безопасности критически важных объектов Уметь:реализовывать с учётом особенностей функционирования критически важных объектов требования нормативно-методической и руководящей документации, а также действующего законодательства по вопросам защиты информации ограниченного доступа Владеть:навыками работы с нормативными правовыми актами в области защиты систем управления критически важных объектов
ПСК-3.3 способностью применять современную нормативную базу, регламентирующую	Знать:нормативно-методические и руководящие документы, регламентирующие обеспечение

<p>деятельность критически важных объектов и обеспечение информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов</p>	<p>информационной безопасности критически важных объектов, способы выявления угроз информационной безопасности на критически важных объектах</p>
	<p>Уметь: реализовывать с учётом особенностей функционирования критически важных объектов требования нормативно-методической и руководящей документации, а также действующего законодательства по вопросам защиты информации ограниченного доступа</p>
<p>ПК-11 способностью разрабатывать политику информационной безопасности автоматизированной системы</p>	<p>Владеть: навыками применения современной нормативной базы для построения системы организационных и программно-технических мер по выявлению, предупреждению и пресечению террористической деятельности в отношении систем управления критически важных объектов</p>
	<p>Знать: нормативно-методические и руководящие документы, регламентирующие обеспечение информационной безопасности критически важных объектов, способы выявления угроз информационной безопасности на критически важных объектах</p>
	<p>Уметь: разрабатывать предложения по совершенствованию и повышению эффективности применения мер информационной безопасности на критически важных объектах</p>
	<p>Владеть: навыками формирования политик безопасности для критически важных объектов и автоматизированных систем критически важных объектов</p>
<p>ОК-5 способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики</p>	<p>Знать: понятие и виды террористической деятельности, основы государственной политики Российской Федерации по противодействию терроризму в информационной сфере, классы и характеристики критически важных объектов</p>
	<p>Уметь:</p>
	<p>Владеть:</p>

3. Место дисциплины в структуре ОП ВО

<p>Перечень предшествующих дисциплин, видов работ учебного плана</p>	<p>Перечень последующих дисциплин, видов работ</p>
<p>Производственная практика (эксплуатационная) (6 семестр)</p>	<p>Не предусмотрены</p>

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

<p>Дисциплина</p>	<p>Требования</p>
<p>Производственная практика (эксплуатационная)</p>	<p>Знает: правовые основы организации защиты</p>

(6 семестр)	государственной тайны и/или конфиденциальной информации; задачи органов защиты государственной тайны и/или служб защиты информации на предприятии, политику безопасности и инструменты администрирования при работе с данными (на рабочих станциях, сервисах, сетях), пользователями, управлением изменениями и обеспечением защищённости и отказоустойчивости администрируемой информационной подсистемы Умеет: анализировать правовые акты и осуществлять правовую оценку информации, циркулирующей в автоматизированной системе, применять политику безопасности и инструменты администрирования при работе с данными (на рабочих станциях, сервисах, сетях), пользователями, управлением изменениями и обеспечением защищённости и отказоустойчивости администрируемой информационной подсистемы Имеет практический опыт: разработки организационно-распорядительных документов по защите информации в автоматизированных системах, применения инструментов администрирования подсистем информационной безопасности автоматизированной системы
-------------	--

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 4 з.е., 144 ч.

Вид учебной работы	Всего часов	Распределение по семестрам	
		в часах	
		Номер семестра	10
Общая трудоёмкость дисциплины	144	144	
<i>Аудиторные занятия:</i>			
Лекции (Л)	36	36	
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	36	36	
Лабораторные работы (ЛР)	0	0	
<i>Самостоятельная работа (СРС)</i>			
Подготовка докладов на семинарах (раздел 5)	14	14	
Подготовка докладов на семинарах (раздел 3)	14	14	
Подготовка докладов на семинарах (раздел 1)	14	14	
Подготовка докладов на семинарах (раздел 4)	14	14	
Подготовка докладов на семинарах (раздел 2)	16	16	
Вид итогового 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	Сущность, причины возникновения и общественная опасность терроризма	12	6	6	0
2	Система противодействия терроризму в Российской Федерации.	20	10	10	0
3	Информационное противоборство. Компьютерные преступления.	12	6	6	0
4	Виды и источники угроз безопасности объектам критической информационной инфраструктуры Российской Федерации	12	6	6	0
5	Обеспечение безопасности систем управления значимых объектов критической информационной инфраструктуры.	16	8	8	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1-2	1	Понятие, виды, условия возникновения и современное состояние терроризма.	4
3	1	Уголовно-процессуальная характеристика преступлений террористического характера.	2
4	2	Организационная основа и принципы противодействия терроризму в Российской Федерации.	2
5-6	2	Силы и средства противодействия терроризму в Российской Федерации.	4
7	2	Организация противодействия терроризму в субъектах Российской Федерации.	2
8	2	Паспорт антитеррористической защищенности предприятия.	2
9	3	Информационные войны и информационное оружие.	2
10	3	Понятие кибертерроризма, виды компьютерных атак.	2
11	3	Уголовно-процессуальная характеристика компьютерных преступлений.	2
12	4	Понятие критической информационной инфраструктуры Российской Федерации. Права и обязанности субъектов критической информационной инфраструктуры.	2
13	4	Порядок категорирования и моделирование угроз безопасности объектов критической информационной инфраструктуры.	2
14	4	Оценка антитеррористической защищенности значимых объектов критической информационной инфраструктуры.	2
15	5	Требования обеспечения безопасности систем управления значимых объектов критической информационной инфраструктуры.	2
16	5	Силы и средства обеспечения безопасности систем управления значимых объектов критической информационной инфраструктуры.	2
17	5	Государственная система обнаружения, предотвращения и ликвидации последствий компьютерных атак (ГосСОПКА) Российской Федерации.	2
18	5	Реагирование на компьютерные инциденты, действия персонала в нештатных ситуациях. Организация взаимодействие подразделений информационной безопасности с ГосСОПКА.	2

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во

			часов
1-2	1	Понятие, виды, условия возникновения и современное состояние терроризма.	4
3	1	Уголовно-процессуальная характеристика преступлений террористического характера.	2
4	2	Организационная основа и принципы противодействия терроризму в Российской Федерации.	2
5-6	2	Силы и средства противодействия терроризму в Российской Федерации.	4
7	2	Организация противодействия терроризму в субъектах Российской Федерации.	2
8	2	Паспорт антитеррористической защищенности предприятия.	2
9	3	Информационные войны и информационное оружие.	2
10	3	Понятие кибертерроризма, виды компьютерных атак.	2
11	3	Уголовно-процессуальная характеристика компьютерных преступлений.	2
12	4	Понятие критической информационной инфраструктуры Российской Федерации. Права и обязанности субъектов критической информационной инфраструктуры.	2
13	4	Порядок категорирования и моделирование угроз безопасности объектов критической информационной инфраструктуры.	2
14	4	Оценка антитеррористической защищенности значимых объектов критической информационной инфраструктуры.	2
15	5	Требования обеспечения безопасности систем управления значимых объектов критической информационной инфраструктуры.	2
16	5	Силы и средства обеспечения информационной безопасности критически важных объектов информационной и телекоммуникационной инфраструктуры	2
17	5	Государственная система обнаружения, предотвращения и ликвидации последствий компьютерных атак (ГосСОПКА) Российской Федерации.	2
18	5	Реагирование на компьютерные инциденты, действия персонала в нештатных ситуациях. Организация взаимодействие подразделений информационной безопасности с ГосСОПКА.	2

5.3. Лабораторные работы

Не предусмотрены

5.4. Самостоятельная работа студента

Выполнение СРС		
Вид работы и содержание задания	Список литературы (с указанием разделов, глав, страниц)	Кол-во часов
Подготовка докладов на семинарах (раздел 2)	1. Лекции преподавателя МПТД (стр. 10-15, 22-27). 2. 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.	16
Подготовка докладов на семинарах (раздел 3)	1. Белоус, А. И. Кибербезопасность объектов топливно-энергетического комплекса. Концепции, методы и средства	14

	обеспечения / А. И. Белоус. — Вологда : Инфра-Инженерия, 2020. Глава 2. Кибероружие - классификация средств и методов применения. 2. 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. 3. Лекции преподавателя МПТД (стр. 15-22).	
Подготовка докладов на семинарах (раздел 1)	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 МПТД (стр. 1-10)	14
Подготовка докладов на семинарах (раздел 5)	1. 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.. 2. 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. 3. ..Лекции преподавателя МПТД (стр. 30-37, 42-45).	14
Подготовка докладов на семинарах (раздел 4)	1. 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. 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 5. Основы поиска уязвимостей программного обеспечения. 3.Лекции преподавателя МПТД (стр. 27-30, 37-42).	14

6. Инновационные образовательные технологии, используемые в учебном процессе

Не предусмотрены

Собственные инновационные способы и методы, используемые в образовательном процессе

Не предусмотрены

Использование результатов научных исследований, проводимых университетом, в рамках данной дисциплины: нет

7. Фонд оценочных средств (ФОС) для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

7.1. Паспорт фонда оценочных средств

Наименование разделов дисциплины	Контролируемая компетенция ЗУНы	Вид контроля (включая текущий)	№№ заданий
Сущность, причины возникновения и общественная опасность терроризма	ОК-5 способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	Выступление с докладом на семинаре (разделы 1), Тестирование (раздел 1)	1
Система противодействия терроризму в Российской Федерации.	ОПК-6 способностью применять нормативные правовые акты в профессиональной деятельности	Выступление с докладом на семинаре (раздел 2), Тестирование (раздел 2)	2
Информационное противоборство. Компьютерные преступления.	ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	Выступление с докладом на семинаре (разделы 3), Тестирование (раздел 3)	3
Виды и источники угроз безопасности объектам критической информационной инфраструктуры Российской Федерации	ПК-11 способностью разрабатывать политику информационной безопасности автоматизированной системы	Выступление с докладом на семинаре (разделы 4), Тестирование (раздел 4)	4
Обеспечение безопасности систем управления значимых объектов критической информационной инфраструктуры.	ПСК-3.3 способностью применять современную нормативную базу, регламентирующую деятельность критически важных объектов и обеспечение информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов	Выступление с докладом на семинаре (разделы 5), Тестирование (раздел 5)	5
Все разделы	ПСК-3.3 способностью применять современную нормативную базу, регламентирующую деятельность критически важных объектов и обеспечение информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов	Бонусное задание	6

Все разделы	ПК-11 способностью разрабатывать политику информационной безопасности автоматизированной системы	Экзамен	7
-------------	--	---------	---

7.2. Виды контроля, процедуры проведения, критерии оценивания

Вид контроля	Процедуры проведения и оценивания	Критерии оценивания
Выступление с докладом на семинаре (разделы 1), Тестирование (раздел 1)	<p>За неделю до семинарского занятия группе задается перечень тем (6-8) для выступления. Время, отведенное на каждое выступление, 10-15 минут. При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Критерии оценки качества доклада.</p> <ol style="list-style-type: none"> 1. Владение профессиональной терминологией: определены все понятия, используемые в докладе – 2 балла; часть понятий не определено, но докладчик смог дать определение, отвечая на дополнительный вопрос - 1 балл; докладчик не знает определения используемых понятий - 0 баллов. 2. Знание нормативно-правовой базы, регламентирующей деятельность по рассматриваемому вопросу: при подготовке доклада студент корректно использовал нормативно-правовые документы из перечня, указанного в разделе курса «Установочная информация» – 1 балл: докладчик использовал утратившие силу нормативно-правовые документы – 0 баллов. 3. Примеры из практики: примеры дополняют и иллюстрируют содержание доклада - 1 балл; примеры не соответствуют теме или отсутствуют - 0 баллов. 4. Вывод о дальнейшем развитии ситуации по рассматриваемой теме: вывод обобщает информацию, использованную в докладе, в нем содержатся субъективные суждения – 1 балл; вывод отсутствует либо не содержит суждений и обобщения – 0. 5. Качество презентации: презентация содержит не только текстовые, но и графические иллюстративные материалы – 2 балла; презентация содержит только тезисы доклада – 1 балл; презентация отсутствует – 0. 6. Ответы на дополнительные вопросы: докладчик уверенно отвечает на поставленные вопросы, демонстрируя владение профессиональной терминологией и знание ранее рассмотренных тем курса - 2 балла; докладчик затрудняется при ответе на дополнительные вопросы -1 балл: 	<p>Зачтено: Рейтинг обучающегося за мероприятие больше или равен 60 %.</p> <p>Не зачтено: Рейтинг обучающегося за мероприятие меньше 60 %.</p>

	<p>докладчик не может ответить ни на один дополнительный вопрос – 0 баллов.</p> <p>Максимальное количество баллов - 9.</p> <p>Весовой коэффициент - 3. По окончании изучения раздела дисциплины проводится тестирование. При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). По окончании изучения раздела дисциплины проводится тестирование, при котором студенту предлагается выбрать правильный ответ на заданный вопрос. Всего необходимо ответить на 10 вопросов в течение 10 минут. Каждый правильный ответ - 1 балл. В случае представления ответа после назначенного времени за каждую минуту вычитается 1 балл.</p> <p>Максимальное количество баллов - 10.</p> <p>Весовой коэффициент - 2.</p>	
Выступление с докладом на семинаре (раздел 2), Тестирование (раздел 2)	<p>За неделю до семинарского занятия группе задается перечень тем (6-8) для выступления. Время, отведенное на каждое выступление, 10-15 минут. При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Критерии оценки качества доклада.</p> <ol style="list-style-type: none"> 1. Владение профессиональной терминологией: определены все понятия, используемые в докладе – 2 балла; часть понятий не определено, но докладчик смог дать определение, отвечая на дополнительный вопрос - 1 балл; докладчик не знает определения используемых понятий - 0 баллов. 2. Знание нормативно-правовой базы, регламентирующей деятельность по рассматриваемому вопросу: при подготовке доклада студент корректно использовал нормативно-правовые документы из перечня, указанного в разделе курса «Установочная информация» – 1 балл; докладчик использовал утратившие силу нормативно-правовые документы – 0 баллов. 3. Примеры из практики: примеры дополняют и иллюстрируют содержание доклада - 1 балл; примеры не соответствуют теме или отсутствуют - 0 баллов. 4. Вывод о дальнейшем развитии ситуации по рассматриваемой теме: вывод обобщает информацию, использованную в докладе, в нем содержатся субъективные 	<p>Зачтено: Рейтинг обучающегося за мероприятие больше или равен 60 %.</p> <p>Не зачтено: Рейтинг обучающегося за мероприятие меньше 60 %.</p>

	<p>суждения – 1 балл; вывод отсутствует либо не содержит суждений и обобщения – 0. 5.</p> <p>Качество презентации: презентация содержит не только текстовые, но и графические иллюстративные материалы – 2 балла; презентация содержит только тезисы доклада – 1 балл; презентация отсутствует – 0. 6. Ответы на дополнительные вопросы: докладчик уверенно отвечает на поставленные вопросы, демонстрируя владение профессиональной терминологией и знание ранее рассмотренных тем курса - 2 балла; докладчик затрудняется при ответе на дополнительные вопросы -1 балл: докладчик не может ответить ни на один дополнительный вопрос – 0 баллов.</p> <p>Максимальное количество баллов - 9.</p> <p>Весовой коэффициент - 3. По окончании изучения раздела дисциплины проводится тестирование. При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). По окончании изучения раздела дисциплины проводится тестирование, при котором студенту предлагается выбрать правильный ответ на заданный вопрос. Всего необходимо ответить на 10 вопросов в течение 10 минут. Каждый правильный ответ - 1 балл. В случае представления ответа после назначенного времени за каждую минуту вычитается 1 балл.</p> <p>Максимальное количество баллов - 10.</p> <p>Весовой коэффициент - 2.</p>	
Выступление с докладом на семинаре (разделы 3), Тестирование (раздел 3)	<p>За неделю до семинарского занятия группе задается перечень тем (6-8) для выступления. Время, отведенное на каждое выступление, 10-15 минут. При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Критерии оценки качества доклада. 1. Владение профессиональной терминологией: определены все понятия, используемые в докладе – 2 балла; часть понятий не определено, но докладчик смог дать определение, отвечая на дополнительный вопрос - 1 балл; докладчик не знает определения используемых понятий - 0 баллов. 2. Знание нормативно-правовой базы, регламентирующей деятельность по</p>	<p>Зачтено: Рейтинг обучающегося за мероприятие больше или равен 60 %.</p> <p>Не зачтено: Рейтинг обучающегося за мероприятие меньше 60 %.</p>

	<p>рассматриваемому вопросу: при подготовке доклада студент корректно использовал нормативно-правовые документы из перечня, указанного в разделе курса «Установочная информация» – 1 балл: докладчик использовал утратившие силу нормативно-правовые документы – 0 баллов. 3. Примеры из практики: примеры дополняют и иллюстрируют содержание доклада - 1 балл; примеры не соответствуют теме или отсутствуют - 0 баллов. 4. Вывод о дальнейшем развитии ситуации по рассматриваемой теме: вывод обобщает информацию, использованную в докладе, в нем содержатся субъективные суждения – 1 балл; вывод отсутствует либо не содержит суждений и обобщения – 0. 5. Качество презентации: презентация содержит не только текстовые, но и графические иллюстративные материалы – 2 балла; презентация содержит только тезисы доклада – 1 балл; презентация отсутствует – 0. 6. Ответы на дополнительные вопросы: докладчик уверенно отвечает на поставленные вопросы, демонстрируя владение профессиональной терминологией и знание ранее рассмотренных тем курса - 2 балла; докладчик затрудняется при ответе на дополнительные вопросы -1 балл: докладчик не может ответить ни на один дополнительный вопрос – 0 баллов. Максимальное количество баллов - 9. Весовой коэффициент - 3. По окончании изучения раздела дисциплины проводится тестирование. При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). По окончании изучения раздела дисциплины проводится тестирование, при котором студенту предлагается выбрать правильный ответ на заданный вопрос. Всего необходимо ответить на 10 вопросов в течение 10 минут. Каждый правильный ответ - 1 балл. В случае представления ответа после назначенного времени за каждую минуту вычитается 1 балл. Максимальное количество баллов - 10. Весовой коэффициент - 2.</p>	
Выступление с докладом на семинаре (разделы 4),	За неделю до семинарского занятия группе задается перечень тем (6-8) для выступления. Время, отведенное на каждое выступление, 10-15 минут. При оценивании	Зачтено: Рейтинг обучающегося за мероприятие больше или равен 60 %. Не зачтено: Рейтинг обучающегося

Тестирование (раздел 4)	<p>результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Критерии оценки качества доклада. 1. Владение профессиональной терминологией: определены все понятия, используемые в докладе – 2 балла; часть понятий не определено, но докладчик смог дать определение, отвечая на дополнительный вопрос - 1 балл; докладчик не знает определения используемых понятий - 0 баллов. 2. Знание нормативно-правовой базы, регламентирующей деятельность по рассматриваемому вопросу: при подготовке доклада студент корректно использовал нормативно-правовые документы из перечня, указанного в разделе курса «Установочная информация» – 1 балл: докладчик использовал утратившие силу нормативно-правовые документы – 0 баллов. 3. Примеры из практики: примеры дополняют и иллюстрируют содержание доклада - 1 балл; примеры не соответствуют теме или отсутствуют - 0 баллов. 4. Вывод о дальнейшем развитии ситуации по рассматриваемой теме: вывод обобщает информацию, использованную в докладе, в нем содержатся субъективные суждения – 1 балл; вывод отсутствует либо не содержит суждений и обобщения – 0. 5. Качество презентации: презентация содержит не только текстовые, но и графические иллюстративные материалы – 2 балла; презентация содержит только тезисы доклада – 1 балл; презентация отсутствует – 0. 6. Ответы на дополнительные вопросы: докладчик уверенно отвечает на поставленные вопросы, демонстрируя владение профессиональной терминологией и знание ранее рассмотренных тем курса - 2 балла; докладчик затрудняется при ответе на дополнительные вопросы -1 балл: докладчик не может ответить ни на один дополнительный вопрос – 0 баллов.</p> <p>Максимальное количество баллов - 9. Весовой коэффициент - 3. По окончании изучения раздела дисциплины проводится тестирование. При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). По</p>	за мероприятие меньше 60 %.
-------------------------	--	-----------------------------

	<p>окончании изучения раздела дисциплины проводится тестирование, при котором студенту предлагается выбрать правильный ответ на заданный вопрос. Всего необходимо ответить на 10 вопросов в течение 10 минут. Каждый правильный ответ - 1 балл. В случае представления ответа после назначенного времени за каждую минуту вычитается 1 балл. Максимальное количество баллов - 10. Весовой коэффициент - 2.</p>	
Выступление с докладом на семинаре (разделы 5), Тестирование (раздел 5)	<p>За неделю до семинарского занятия группе задается перечень тем (6-8) для выступления. Время, отведенное на каждое выступление, 10-15 минут. При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Критерии оценки качества доклада. 1. Владение профессиональной терминологией: определены все понятия, используемые в докладе – 2 балла; часть понятий не определено, но докладчик смог дать определение, отвечая на дополнительный вопрос - 1 балл; докладчик не знает определения используемых понятий - 0 баллов. 2. Знание нормативно-правовой базы, регламентирующей деятельность по рассматриваемому вопросу: при подготовке доклада студент корректно использовал нормативно-правовые документы из перечня, указанного в разделе курса «Установочная информация» – 1 балл: докладчик использовал утратившие силу нормативно-правовые документы – 0 баллов. 3. Примеры из практики: примеры дополняют и иллюстрируют содержание доклада - 1 балл; примеры не соответствуют теме или отсутствуют - 0 баллов. 4. Вывод о дальнейшем развитии ситуации по рассматриваемой теме: вывод обобщает информацию, использованную в докладе, в нем содержатся субъективные суждения – 1 балл; вывод отсутствует либо не содержит суждений и обобщения – 0. 5. Качество презентации: презентация содержит не только текстовые, но и графические иллюстративные материалы – 2 балла; презентация содержит только тезисы доклада – 1 балл; презентация отсутствует – 0. 6. Ответы на дополнительные вопросы: докладчик уверенно отвечает на поставленные вопросы, демонстрируя владение</p>	<p>Зачтено: Рейтинг обучающегося за мероприятие больше или равен 60 %. Не зачтено: Рейтинг обучающегося за мероприятие меньше 60 %.</p>

	<p>профессиональной терминологией и знание ранее рассмотренных тем курса - 2 балла; докладчик затрудняется при ответе на дополнительные вопросы -1 балл: докладчик не может ответить ни на один дополнительны вопрос – 0 баллов.</p> <p>Максимальное количество баллов - 9.</p> <p>Весовой коэффициент - 3. По окончании изучения раздела дисциплины проводится тестирование. При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). По окончании изучения раздела дисциплины проводится тестирование, при котором студенту предлагается выбрать правильный ответ на заданный вопрос. Всего необходимо ответить на 10 вопросов в течение 10 минут. Каждый правильный ответ - 1 балл. В случае представления ответа после назначенного времени за каждую минуту вычитается 1 балл.</p> <p>Максимальное количество баллов - 10.</p> <p>Весовой коэффициент - 2.</p>	
Бонусное задание	<p>Студент представляет копии документов, подтверждающие победу или участие в конференции, а также копии документов, подтверждающие наличие публикации, проиндексированной в международной базе данных (Scopus, Web of Science), РИНЦ или в издании, входящем в перечень ВАК.. При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Максимально возможная величина бонус-рейтинга +15 %.</p>	<p>Зачтено: 15% за победу во всероссийской конференции и/или участие в международной конференции и наличие публикации, проиндексированной в международной базе данных (Scopus, Web of Science); 12% за призовое место на всероссийской конференции и наличие публикации в журнале ВАК;</p> <p>10% за призовое место на всероссийской конференции и наличие публикации, проиндексированной в РИНЦ;</p> <p>6% за участие во всероссийской конференции или победу в университетской конференции и наличие публикации, проиндексированной в РИНЦ;</p> <p>4% за призовое место на университетской конференции и наличие публикации, проиндексированной в РИНЦ;</p> <p>2% за участие в университетской конференции и наличие публикации, проиндексированной в РИН;</p> <p>3% за отсутствие пропусков занятий без уважительной причины.</p>

		Не зачтено: не предусмотрено
Экзамен	<p>На экзамене происходит оценивание учебной деятельности обучающихся по дисциплине на основе полученных оценок за контрольно-рейтинговые мероприятия текущего контроля и промежуточной аттестации. 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) Студенты в аудитории письменно отвечают на вопросы экзаменационного билета, который включает 2 теоретических вопроса по пройденным разделам, преподаватель проверяет, беседует и оценивает.</p> <p>Показатели оценивания ответов по каждому из вопросов: 6 баллов – студент обладает твёрдым и полным знанием материала дисциплины, владеет дополнительными знаниями, даны полные, развёрнутые ответы; логически, грамотно и точно излагает материал дисциплины, интерпретируя его самостоятельно, способен самостоятельно его анализировать и делать выводы 5 баллов – студент знает материал дисциплины в запланированном объёме, некоторые моменты в ответе не отражены или в ответе имеются несущественные неточности; грамотно и по существу излагает материал.</p> <p>3 балла – студент знает только основной материал дисциплины, не усвоил его деталей, дана только часть ответа на вопросы; в ответе имеются существенные ошибки; допускает неточности в изложении и интерпретации знаний; имеются нарушения логической последовательности 0 баллов – студент не знает значительной части материала дисциплины; ответ не дан или допускает грубые ошибки при изложении ответа на вопрос; неверно излагает и интерпретирует знания; изложение материала логически не выстроено. Максимальное количество баллов - 12.</p>	<p>Отлично: величина рейтинга обучающегося по дисциплине 85...100 %</p> <p>Хорошо: величина рейтинга обучающегося по дисциплине 75...84 %</p> <p>Удовлетворительно: величина рейтинга обучающегося по дисциплине 60...74 %</p> <p>Неудовлетворительно: величина рейтинга обучающегося по дисциплине 0...59 %</p>

7.3. Типовые контрольные задания

Вид контроля	Типовые контрольные задания
Выступление с докладом на семинаре (разделы 1), Тестирование (раздел 1)	Доклады на семинар (раздел 1).docx; Пример

	тестового задания (раздел 1).docx
Выступление с докладом на семинаре (раздел 2), Тестирование (раздел 2)	Доклады на семинар (раздел 2).docx; Пример тестового задания (раздел 2).docx
Выступление с докладом на семинаре (разделы 3), Тестирование (раздел 3)	Доклады на семинар (раздел 3).docx; Пример тестового задания (раздел 3).docx
Выступление с докладом на семинаре (разделы 4), Тестирование (раздел 4)	Пример тестового задания (раздел 4).docx; Доклады на семинар (раздел 4).docx
Выступление с докладом на семинаре (разделы 5), Тестирование (раздел 5)	Доклады на семинар (раздел 5).docx; Пример тестового задания (раздел 5).docx
Бонусное задание	
Экзамен	Система оценок..docx

8. Учебно-методическое и информационное обеспечение дисциплины

Печатная учебно-методическая документация

а) основная литература:

Не предусмотрена

б) дополнительная литература:

1. Закиров, Р. Ш. Информационная безопасность [Текст] конспект лекций по направлениям подготовки "Экономика" и "Менеджмент" Р. Ш. Закиров ; Юж.-Урал. гос. ун-т, Каф. Экономика и упр. проектами ; ЮУрГУ. - Челябинск: Издательский Центр ЮУрГУ, 2014. - 72, [1] с. электрон. версия

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

Не предусмотрены

г) методические указания для студентов по освоению дисциплины:

1. Лекции преподавателя МПТД

из них: учебно-методическое обеспечение самостоятельной работы студента:

1. Лекции преподавателя МПТД

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 : электронно-библиотечная система. — URL: https://e.lanbook.com/book/167606
2	Основная	Электронно-	Белоус, А. И. Кибербезопасность объектов топливно-

	литература	библиотечная система издательства Лань	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. 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. — URL: https://e.lanbook.com/book/131717

9. Информационные технологии, используемые при осуществлении образовательного процесса

Перечень используемого программного обеспечения:

Нет

Перечень используемых информационных справочных систем:

Нет

10. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Лекции	912 (3б)	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+ .
Практические занятия и семинары	912 (3б)	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+ .