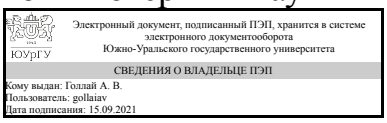
ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Директор института
Высшая школа электроники и компьютерных наук



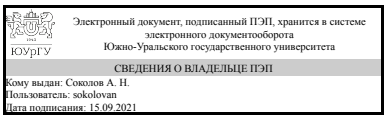
А. В. Голлай

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

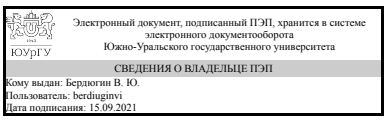
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем, утверждённым приказом Минобрнауки от 01.12.2016 № 1509

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



А. Н. Соколов

Разработчик программы,
доцент



В. Ю. Бердюгин

Челябинск

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-11 способностью разрабатывать политику 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:разрабатывать предложения по совершенствованию и повышению эффективности применения мер информационной безопасности на критически важных объектах
	Владеть:навыками формирования политик 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

	Знать:нормативно-методические и руководящие документы, регламентирующие обеспечение информационной безопасности критически важных объектов, способы выявления угроз информационной безопасности на критически важных объектах
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	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 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
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	Знать:понятие и виды террористической деятельности, основы государственной политики Российской Федерации по противодействию терроризму в информационной сфере, классы и характеристики и критически важных объектов
	Уметь:
	Владеть:
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

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Б.1.17 Основы информационной безопасности, Б.1.21 Программно-аппаратные средства обеспечения информационной безопасности, Б.1.26 Управление информационной безопасностью	Не предусмотрены

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

Дисциплина	Требования
Б.1.21 Программно-аппаратные средства обеспечения информационной безопасности	знать: программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях; уметь: проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы; разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем; владеть::навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности; навыками использования программно-аппаратных средств обеспечения безопасности сетей ЭВМ.
Б.1.26 Управление информационной безопасностью	знать: подходы к формированию систем информационной безопасности предприятий и организаций, их элементный состав; содержание основных документов, регламентирующих правила эксплуатации и технического обслуживания средств защиты информации с учетом требований охраны труда и техники безопасности; уметь: применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности; организовать мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации; владеть: навыками разработки предложений по совершенствованию систем информационной безопасности предприятий и организаций, комплексно обеспечивающих повышение ее уровня.
Б.1.17 Основы информационной безопасности	знать: основные термины по проблематике информационной безопасности; цели, задачи, принципы и основные направления обеспечения информационной безопасности; место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России; содержание информационной войны, методы и средства ее ведения; источники и классификацию угроз информационной безопасности; основные средства и способы обеспечения информационной безопасности,

	принципы построения систем защиты информации; уметь: классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; владеть: профессиональной терминологией в области информационной безопасности.

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
Аудиторные занятия:	72	72
Лекции (Л)	36	36
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	36	36
Лабораторные работы (ЛР)	0	0
Самостоятельная работа (СРС)	72	72
Изучение, конспектирование нормативных правовых актов, монографий, учебных пособий, периодических изданий	18	18
Написание тематических докладов, рефератов и эссе на проблемные темы	36	36
Подготовка к экзамену	18	18
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	8	4	4	0
2	Основные черты современного терроризма	12	6	6	0
3	Система противодействия терроризму в Российской Федерации и мире	12	6	6	0
4	Критически важные объекты и системы управления ими	16	8	8	0
5	Обеспечение безопасности критически важных объектов информационной и телекоммуникационной инфраструктуры	12	6	6	0
6	Средства противодействия террористической деятельности в системах управления критически важных объектов	12	6	6	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов

1	1	Понятие и виды терроризма	2
2	1	Терроризм и борьба с ним в исторической ретроспективе	2
3	2	Условия возникновения и современное состояние терроризма	2
4	2	Виды международных террористических организаций. Особенности современного терроризма в России.	2
5	2	Информационные технологии как объект терроризма	2
6	3	Система противодействия терроризму в Российской Федерации	2
7	3	Система противодействия терроризму за рубежом	2
8	3	Международное сотрудничество в борьбе с терроризмом	2
9	4	Критически важные объекты	2
10	4	Паспорт антитеррористической защищенности критически важного объекта	2
11	4	Средства обеспечения мониторинга безопасности критически важных объектов	2
12	4	Системы управления критически важными объектами	2
13	5	Основные принципы государственной политики в области обеспечения безопасности критически важных объектов	2
14	5	Обеспечение информационной безопасности критически важных объектов информационной и телекоммуникационной инфраструктуры	2
15	5	Понятие и виды кибертерроризма	2
16	6	Силы, средства и системы обеспечения информационной безопасности критически важных объектов	2
17	6	Предотвращение компьютерных атак., защита автоматизированных систем управления и их компонентов, аудит безопасности систем управления критически важных объектов	2
18	6	Реагирование на компьютерные инциденты, действия персонала в нештатных ситуациях	2

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	1	Понятие и виды терроризма	2
2	1	Терроризм и борьба с ним в исторической ретроспективе	2
3	2	Условия возникновения и современное состояние терроризма	2
4	2	Виды международных террористических организаций. Особенности современного терроризма в России.	2
5	2	Информационные технологии как объект терроризма	2
6	3	Система противодействия терроризму в Российской Федерации	2
7	3	Система противодействия терроризму за рубежом	2
8	3	Международное сотрудничество в борьбе с терроризмом	2
9	4	Критически важные объекты	2
10	4	Паспорт антитеррористической защищенности критически важного объекта	2
11	4	Средства обеспечения мониторинга безопасности критически важных объектов	2
12	4	Системы управления критически важными объектами	2
13	5	Основные принципы государственной политики в области обеспечения безопасности критически важных объектами	2
14	5	Обеспечение информационной безопасности критически важных объектов информационной и телекоммуникационной инфраструктуры	2
15	5	Понятие и виды кибертерроризма	2

16	6	Силы, средства и системы обеспечения информационной безопасности критически важных объектов	2
17	6	Предотвращение компьютерных атак., защита автоматизированных систем управления и их компонентов, аудит безопасности систем управления критически важных объектов	2
18	6	Реагирование на компьютерные инциденты, действия персонала в нештатных ситуациях	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
Написание тематических докладов, рефератов и эссе на проблемные темы	1	36
Изучение, конспектирвание нормативных правовых актов, монографий, учебных пособий, периодических изданий	1	18
Подготовка к экзамену	1	18

6. Инновационные образовательные технологии, используемые в учебном процессе

Инновационные формы учебных занятий	Вид работы (Л, ПЗ, ЛР)	Краткое описание	Кол-во ауд. часов
деловая игра	Практические занятия и семинары	студенты распределяются по ролям: одни организовывают физическую охрану объекта, другие должны найти уязвимые места чтобы проникнуть на объект	2

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
Все разделы	ПК-4 способностью разрабатывать	экзамен	Вопросы

	модели угроз и модели нарушителя информационной безопасности автоматизированной системы		билетов.
Все разделы	ПК-11 способностью разрабатывать политику информационной безопасности автоматизированной системы	экзамен	Вопросы билетов.
Все разделы	ОПК-6 способностью применять нормативные правовые акты в профессиональной деятельности	экзамен	Вопросы билетов.
Система противодействия терроризму в Российской Федерации и мире	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.	Темы докладов №1
Обеспечение безопасности критически важных объектов информационной и телекоммуникационной 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 на семинаре.	Темы докладов №2
Все разделы	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	Бонусное задание	Не требуется.

7.2. Виды контроля, процедуры проведения, критерии оценивания

Вид контроля	Процедуры проведения и оценивания	Критерии оценивания
экзамен	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. Показатели оценивания	Отлично: величина рейтинга обучающегося по дисциплине 85…100 % Хорошо: величина рейтинга обучающегося по дисциплине 75…84 % Удовлетворительно: величина рейтинга обучающегося по дисциплине 60…74 % Неудовлетворительно: величина рейтинга обучающегося по дисциплине 0…59 %

	ответов по каждому из вопросов: 3 балла – 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 2 балла – 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. 1 балл – 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	
Выступление с докладом на семинаре.	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: полнота – объем знаний по рассматриваемому вопросу; конкретность – умение раскрыть конкретные проявления обобщённых знаний (доказать на примерах основные положения); системность – представление знаний по теме, с выделением структурных её элементов, расположенных в логической последовательности; осознанность – понимание связей между знаниями, умение выделить существенные и несущественные связи, познание способов и принципов получения знаний. Доклад полностью соответствующий перечисленным критериям соответствует 2 баллам. Частично соответствующий - 1 баллу. Не соответствующий - 0 баллов. Максимальное количество баллов – 10.	Зачтено: Рейтинг обучающегося за мероприятие больше или равен 60 %. Не зачтено: Рейтинг обучающегося за мероприятие меньше 60 %.
Бонусное задание	Отмечается присутствие студента на занятиях. В случае отсутствия пропусков по уважительной причине студент получает дополнительные баллы. Максимальное количество баллов за семестр равно 3	Зачтено: Рейтинг обучающегося за мероприятие равен 100 %. Не зачтено: Рейтинг обучающегося за мероприятие меньше 100 %.

7.3. Типовые контрольные задания

Вид контроля	Типовые контрольные задания
экзамен	

	Вопросы билетов МПТД.docx
Выступление с докладом на семинаре.	Темы докладов на семинарах..docx
Бонусное задание	

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:

г) методические указания для студентов по освоению дисциплины:

1. Лекции преподавателя

из них: учебно-методическое обеспечение самостоятельной работы студента:

2. Лекции преподавателя

Электронная учебно-методическая документация

№	Вид литературы	Наименование разработки	Наименование ресурса в электронной форме	Доступность (сеть Интернет / локальная сеть; авторизованный / свободный доступ)
1	Основная литература	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	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный
2	Дополнительная литература	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	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный

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
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, Mozila Firefox, Консультант+ .
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, Mozila Firefox, Консультант+ .