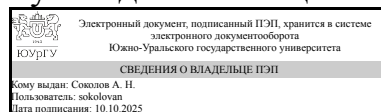


ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Руководитель специальности



А. Н. Соколов

РАБОЧАЯ ПРОГРАММА

дисциплины 1.О.37 Контроль защищенности автоматизированных систем
для специальности 10.05.03 Информационная безопасность автоматизированных систем

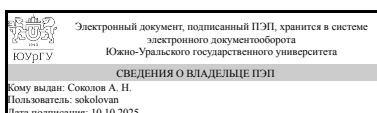
уровень Специалитет

форма обучения очная

кафедра-разработчик Защита информации

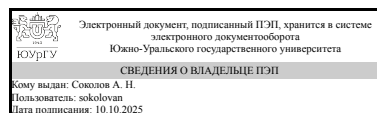
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем, утвержденным приказом Минобрнауки от 26.11.2020 № 1457

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



А. Н. Соколов

Разработчик программы,
к.техн.н., доц., заведующий
кафедрой



А. Н. Соколов

1. Цели и задачи дисциплины

Целью дисциплины является подготовка квалифицированных специалистов способных осуществить контроль безопасности информационных ресурсов и систем при катастрофах, авариях, стихийных бедствиях и их последствиях. Задачами дисциплины являются: изучение основ и методов поиска рациональных решений построения катастрофоустойчивых информационных систем; изучение основных подходов к обеспечению информационной безопасности катастрофоустойчивых информационных систем; изучение принципов функционирования современных средств построения и аппаратно-программных платформ построения информационных систем; приобретение студентами навыков по проектированию и реализации комплекса мер, обеспечивающих информационную безопасность в условиях чрезвычайных ситуаций, минимизации последствий чрезвычайных ситуаций и вывода информационной системы на заданный уровень.

Краткое содержание дисциплины

В течение дисциплины студентами будут изучены такие темы как: виды чрезвычайных ситуаций и их возможные последствия; вопросы проектирование катастрофоустойчивых информационных систем; разработка комплекса мер по реализации проектов катастрофоустойчивых информационных систем; ликвидация последствий чрезвычайных ситуаций в работе информационных систем.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине
ОПК-15 Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем	Знает: руководящие и методические документы уполномоченных федеральных органов исполнительной власти по обеспечению безопасности информации в автоматизированных системах; способы обеспечения контроля защищенности автоматизированных систем Умеет: осуществлять планирование и организацию контроля защищенности автоматизированной системы с учетом требований по защите информации; проводить диагностику и мониторинг систем защиты автоматизированных систем Имеет практический опыт: разработки документов для обеспечения контроля защищенности информации в автоматизированной системе при её эксплуатации (включая управление инцидентами информационной безопасности); применения способов обеспечения контроля защищенности автоматизированных систем

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
1.О.34 Безопасность систем баз данных, 1.О.32 Безопасность сетей электронных вычислительных машин, 1.О.35 Информационная безопасность открытых систем, 1.О.33 Безопасность операционных систем, ФД.02 Мониторинг информационной безопасности и активный поиск киберугроз	1.О.47 Измерительная аппаратура контроля защищенности объектов информатизации

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

Дисциплина	Требования
1.О.35 Информационная безопасность открытых систем	Знает: принципы формирования политики информационной безопасности в автоматизированных системах , риски подсистем защиты информации автоматизированных систем и экспериментальные методы их оценки Умеет: разрабатывать частные политики информационной безопасности автоматизированных систем , анализировать и оценивать угрозы информационной безопасности автоматизированных систем Имеет практический опыт: управления процессами обеспечения безопасности автоматизированных систем, анализа информационной инфраструктуры автоматизированных систем
1.О.33 Безопасность операционных систем	Знает: устройство и принципы работы операционных систем, структуру и возможности подсистем защиты операционных систем семейств UNIX и Windows, методы администрирования и принципы работы операционных систем семейств UNIX и Windows Умеет: использовать средства управления работой операционной системы; формулировать политику безопасности операционных систем семейств UNIX и Windows, настраивать политику безопасности операционных систем семейств UNIX и Windows Имеет практический опыт: установки операционных систем семейств Windows и Unix, администрирования операционных систем семейств Windows и Unix с учетом требований по обеспечению информационной безопасности
1.О.32 Безопасность сетей электронных вычислительных машин	Знает: методы администрирования вычислительных сетей, методы проектирования вычислительных сетей Умеет: администрировать вычислительные сети; реализовывать политику безопасности вычислительной сети, проектировать вычислительные сети Имеет практический опыт: администрирования

	локальных вычислительных сетей с учетом требований по обеспечению информационной безопасности, эксплуатации локальных вычислительных сетей
1.О.34 Безопасность систем баз данных	Знает: средства обеспечения безопасности данных, назначение, функции и структуру систем управления базами данных Умеет: администрировать базы данных, эксплуатировать базы данных;создавать объекты базы данных;выполнять запросы к базе данных;разрабатывать прикладные программы, осуществляющие взаимодействие с базами данных Имеет практический опыт: администрирования баз данных с учетом требований по обеспечению информационной безопасности, эксплуатации баз данных с учетом требований по обеспечению информационной безопасности
ФД.02 Мониторинг информационной безопасности и активный поиск киберугроз	Знает: методы мониторинга информационной безопасности и средства реализации удаленных сетевых атак на автоматизированные системы, организационную структуру и функциональную часть автоматизированных систем; методы и средства реализации удаленных сетевых атак на автоматизированные системы Умеет: осуществлять диагностику и мониторинг систем защиты автоматизированных систем, осуществлять управление и администрирование защищенных автоматизированных систем; разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем Имеет практический опыт: разработки политик информационной безопасности автоматизированных систем

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 2 з.е., 72 ч., 40,25 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		8
Общая трудоёмкость дисциплины	72	72
<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>	31,75	31,75
Составление технического задания на разработку	31,75	31.75

катастрофоустойчивой информационной системы		
Консультации и промежуточная аттестация	4,25	4,25
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	Катастрофоустойчивость в системе национальной безопасности Российской Федерации	4	4	0	0
2	Методы обеспечения катастрофоустойчивости автоматизированных систем	12	8	4	0
3	Средства и практические решения по обеспечению катастрофоустойчивости ав-томатизированных систем	12	8	4	0
4	Организация функционирования катастрофоустойчивых автоматизированных систем	8	4	4	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол- во часов
1	1	Национальные интересы и угрозы катастрофоустойчивости Российской Федерации в информационной сфере и их обеспечение	4
2	2	Обеспечение катастрофоустойчивости системы	4
3	2	Выбор рациональных решений по организации средств восстановления информационных систем после отказов и катастроф и Оптимизация средств восстановления после отказов	4
4	3	Практические решения построения средств восстановления после катастроф	2
5	3	Основы обеспечения информационной безопасности в катастрофоустойчивых центрах обработки информации	4
6	3	Принципы построения организационно-режимных мер обеспечения безопасности информации	2
7	4	Организационно-технические решения по обеспечению защиты от несанкционированного доступа со стороны обслуживающего персонала к ресурсам ИС в особых режимах ее функционирования	2
8	4	Типовой сценарий переноса обработки в случае частичного или полного выхода из строя центра обработки информации	2

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол- во часов
1	1	Понятие национальной безопасности; Виды защищаемой информации	0
2	2	Расчет показателей доступности информационно-телекоммуникационных систем	2
3	2	Методы обеспечения катастрофоустойчивости	2
4	3	Средства обеспечения катастрофоустойчивости	2
5	3	Разработка технического задания на катастрофоустойчивые системы	2
6	4	Организация работ по развертыванию катастрофоустойчивых решений.	2

7	4	Планы восстановления после катастроф.	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
Составление технического задания на разработку катастрофоустойчивой информационной системы	Катастрофоустойчивость информационных систем [Текст : непосредственный] : учеб. пособие по направлению 10.03.01 и др. / В. М. Жернова, Н. В. Плотникова ; Юж.-Урал. гос. ун-т, Каф. Кафедра Защита информации ; ЮУрГУ Челябинск : Издательский Центр ЮУрГУ , 2020	8	31,75

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	8	Текущий контроль	Практическая работа №1	1	14	Выполнены все критерии практической работы - 14 баллов. За каждый невыполненный критерий не начисляются 2 балла	зачет
2	8	Текущий контроль	Практическая работа №2	1	14	Выполнены все критерии практической работы - 14 баллов. За каждый невыполненный критерий не начисляются 2 балла	зачет
3	8	Текущий контроль	Практическая работа №3	1	14	Выполнены все критерии практической работы - 14 баллов. За каждый невыполненный критерий не начисляются 2 балла	зачет
4	8	Текущий контроль	Практическая работа №4	1	14	Выполнены все критерии практической работы - 14 баллов. За каждый невыполненный критерий не начисляются 2 балла	зачет
5	8	Текущий контроль	Практическая работа №5	1	14	Выполнены все критерии практической работы - 14 баллов. За каждый невыполненный критерий не	зачет

						начисляются 2 балла	
6	8	Текущий контроль	Практическая работа №6	1	14	Выполнены все критерии практической работы - 14 баллов. За каждый невыполненный критерий не начисляются 2 балла	зачет
7	8	Бонус	Посещаемость	-	1	Посещено более 60% лекционных И 60% практических занятий - начисляется 1 балл, в противном случае - 0 баллов	зачет
8	8	Промежуточная аттестация	Тест на зачет	-	15	Зачтено: 9 и более правильных ответов Не зачтено: 6 и менее правильных ответов	зачет

6.2. Процедура проведения, критерии оценивания

Вид промежуточной аттестации	Процедура проведения	Критерии оценивания
зачет	тест на зачете - 15 баллов, каждая из 6 практических работ по 14 баллов (итого 84), 1 балл - бонус за посещение занятий. Итого 100 баллов. Зачтено при условии, что набрано минимум 60% по каждому из мероприятий - т.е. не менее 60% на зачете и не менее 60% по каждой из практических работ	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	8
ОПК-15	Знает: руководящие и методические документы уполномоченных федеральных органов исполнительной власти по обеспечению безопасности информации в автоматизированных системах; способы обеспечения контроля защищенности автоматизированных систем	++						++	
ОПК-15	Умеет: осуществлять планирование и организацию контроля защищенности автоматизированной системы с учетом требований по защите информации; проводить диагностику и мониторинг систем защиты автоматизированных систем				++			++	
ОПК-15	Имеет практический опыт: разработки документов для обеспечения контроля защищенности информации в автоматизированной системе при её эксплуатации (включая управление инцидентами информационной безопасности); применения способов обеспечения контроля защищенности автоматизированных систем						+++		

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:

1. Журнал "Вестник УРФО. Безопасность в информационной сфере"

г) методические указания для студентов по освоению дисциплины:

1. Катастрофоустойчивость информационных систем [Текст : непосредственный] : учеб. пособие по направлению 10.03.01 и др. / В. М. Жернова, Н. В. Плотникова ; Юж.-Урал. гос. ун-т, Каф. Кафедра Защита информации ; ЮУрГУ Челябинск : Издательский Центр ЮУрГУ , 2020

из них: учебно-методическое обеспечение самостоятельной работы студента:

1. Катастрофоустойчивость информационных систем [Текст : непосредственный] : учеб. пособие по направлению 10.03.01 и др. / В. М. Жернова, Н. В. Плотникова ; Юж.-Урал. гос. ун-т, Каф. Кафедра Защита информации ; ЮУрГУ Челябинск : Издательский Центр ЮУрГУ , 2020

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
1	Основная литература	Электронный каталог ЮУрГУ	Катастрофоустойчивость информационных систем [Текст : непосредственный] : учеб. пособие по направлению 10.03.01 и др. / В. М. Жернова, Н. В. Плотникова ; Юж.-Урал. гос. ун-т, Каф. Кафедра Защита информации ; ЮУрГУ Челябинск : Издательский Центр ЮУрГУ , 2020 https://lib.susu.ru/ftd?base=SUSU_METHOD1&key=000568292&dtype=F&ety

Перечень используемого программного обеспечения:

1. Microsoft-Office(бессрочно)

Перечень используемых профессиональных баз данных и информационных справочных систем:

1. ООО "ГарантУралСервис"-Гарант(31.12.2022)

8. Материально-техническое обеспечение дисциплины

Не предусмотрено