ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Руководитель специальности

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Соколов А. Н.
Пользователь: sokolovan
Дата подписания: 24.12.2022

А. Н. Соколов

РАБОЧАЯ ПРОГРАММА

дисциплины 1.О.39 Контроль безопасности 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, утверждённым приказом Минобрнауки от 26.11.2020 № 1457

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

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Соколов А. Н.
Пользователь: sokolovan
Дата подписания: 24.12.2022

А. Н. Соколов

Разработчик программы,
к.юрид.н., доцент

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Жернова В. М.
Пользователь: zhernovavm
Дата подписания: 24.12.2022

В. М. Жернова

Челябинск

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 катастофоустойчивых 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 выведения 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-13 Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем	Знает: руководящие и методические документы уполномоченных федеральных органов исполнительной власти по обеспечению безопасности информации в автоматизированных системах Умеет: осуществлять планирование, организацию и контроль работы персонала автоматизированной системы с учетом требований по защите информации Имеет практический опыт: разработки документов для обеспечения контроля безопасности информации в автоматизированной системе при её эксплуатации (включая управление инцидентами информационной безопасности)

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
ФД.02 Мониторинг информационной безопасности и активный поиск киберугроз, 1.О.30 Защита информации от утечки по техническим каналам,	1.О.38.02 Эксплуатация автоматизированных систем в защищенном исполнении

1.О.36 Информационная безопасность открытых систем	

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

Дисциплина	Требования
1.О.36 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.30 Защита информации от утечки по техническим каналам	Знает: классификацию и количественные характеристики технических каналов утечки информации;способы и средства защиты информации от утечки по техническим каналам, контроля их эффективности;организацию защиты информации от утечки по техническим каналам на объектах информатизации, типовые методики проведения измерений параметров, характеризующих наличие технических каналов утечки информации Умеет: использовать средства инструментального контроля показателей эффективности технической защиты информации, проводить контрольно-измерительные работы в целях оценки количественных характеристик технических каналов утечки информации Имеет практический опыт: проектирования системы защиты объекта информатизации от утечек по техническим каналам
ФД.02 Мониторинг информационной безопасности и активный поиск киберугроз	Знает: организационную структуру и функциональную часть автоматизированных систем; методы и средства реализации удаленных сетевых атак на автоматизированные системы, методы мониторинга информационной безопасности и средства реализации удаленных сетевых атак на автоматизированные системы Умеет: осуществлять управление и администрирование защищенных автоматизированных систем; разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем, осуществлять диагностику и мониторинг систем защиты 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
Аудиторные занятия:	36	36
Лекции (Л)	24	24
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	12	12
Лабораторные работы (ЛР)	0	0
Самостоятельная работа (СРС)	31,75	31,75
Составление технического задание на разработку катастрофоустойчивой информационной системы	31,75	31.75
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 катстрофоустойчивых 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 задание 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	Учи-тыва-ется 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 начисляются 2 балла	зачет
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	Проме-жуточная 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-13	Знает: руководящие и методические документы уполномоченных федеральных органов исполнительной власти по обеспечению безопасности информации в автоматизированных системах	+	+	+					

ОПК-13	Умеет: осуществлять планирование, организацию и контроль работы персонала автоматизированной системы с учетом требований по защите информации		+						
ОПК-13	Имеет практический опыт: разработки документов для обеспечения контроля безопасности информации в автоматизированной системе при её эксплуатации (включая управление инцидентами информационной безопасности)								+

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 : непосредст учеб. пособие по направлению 10.03.01 и др. / В. М. Жернова, Н. В. Пл Юж.-Урал. гос. ун-т, Каф. Кафедра Защита информации ; ЮУрГУ Челя Издательский Центр ЮУрГУ , 2020 https://lib.susu.ru/ftd?base=SUSU_METHOD1&key=000568292&dtype=F
2	Дополнительная литература	Электронно-библиотечная система издательства Лань	Тумбинская, М. В. Защита информации на предприятии : учебное посо Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2020. — 18 ISBN 978-5-8114-4291-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/130184 (дата обращения: 25.01.2022). — Режим доступа: для авториз. пользователей
3	Основная	Электронно-	Фот, Ю. Д. Стандарты информационной безопасности : учебное пособ

	литература	библиотечная система издательства Лань	Фот. — Оренбург : ОГУ, 2018. — 226 с. — ISBN 978-5-7410-2297-9. — электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/159804 (дата обращения: 22.09.2021). — Реж для авториз. пользователей.
4	Дополнительная литература	Электронно-библиотечная система издательства Лань	Паршин, К. А. Методы и средства проектирования информационных с технологий : учебно-методическое пособие / К. А. Паршин. — Екатери 2018. — 129 с. — Текст : электронный // Лань : электронно-библиотечн — URL: https://e.lanbook.com/book/121337 (дата обращения: 25.01.2022 доступа: для авториз. пользователей.

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