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: 11.06.2023

А. Н. Соколов

РАБОЧАЯ ПРОГРАММА

дисциплины 1.Ф.10 Математическое моделирование информационных потоков и систем защиты информации
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: 11.06.2023

А. Н. Соколов

Разработчик программы,
д.физ.-мат.н., доц., профессор

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Зюляркина Н. Д.
Пользователь: ziuliarkinand
Дата подписания: 08.06.2023

Н. Д. Зюляркина

Челябинск

1. Цели и задачи дисциплины

Целью дисциплины является ознакомление обучаемых с методами моделирования защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации. Задачами дисциплины являются: - изучение основных видов математических моделей информационных потоков и систем защиты информации и методы их построения; - изучение методов, позволяющих на основе опытных данных и технических характеристик автоматизированной системы управления (АСУ) строить адекватную математическую модель, связанную с системой защиты информации в АСУ

Краткое содержание дисциплины

Студенты изучают основных виды математических моделей информационных потоков и систем защиты информации и методы их построения и методы, позволяющие на основе опытных данных и технических характеристик автоматизированной системы управления (АСУ) строить адекватную математическую модель, связанную с системой защиты информации в АСУ

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине
ПК-1 Способен моделировать защищенные автоматизированные системы с целью анализа их уязвимостей и эффективности средств и способов защиты информации	Знает: основные виды математических моделей информационных потоков и систем защиты информации и методы их построения Умеет: на основе опытных данных и технических характеристик автоматизированной системы управления (АСУ) строить адекватную математическую модель, связанную с системой защиты информации в АСУ Имеет практический опыт: применения математических моделей для построения системы защиты информации в АСУ и оценки ее эффективности

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
1.Ф.01 Автоматизированные системы управления, 1.Ф.02 Современные киберугрозы в промышленных и корпоративных системах автоматизации, 1.Ф.05 Кодирование информации в автоматизированных системах управления	Не предусмотрены

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

Дисциплина	Требования
1.Ф.01 Автоматизированные системы управления	Знает: цели и задачи автоматизации управления, общие понятия автоматизированных систем управления (АСУ), жизненный цикл, функции и виды АСУ;состав автоматизированных систем управления технологическим процессом (АСУ ТП), виды обеспечения, классификацию и уровни управления АСУ ТП, место АСУ ТП в интегрированных системах управления, архитектуру промышленных сетей АСУ ТП Умеет: анализировать и моделировать информационные процессы, протекающие в системах промышленной автоматизации, применять методы и средства регистрации, записи и хранения значимых параметров потоков данных АСУ ТП Имеет практический опыт: определения ключевых точек мониторинга значимых параметров потоков данных, распределенных в информационной системе промышленных сетей АСУ ТП
1.Ф.05 Кодирование информации в автоматизированных системах управления	Знает: основные способы кодирования информации в автоматизированных системах управления (АСУ), обеспечивающие максимальную надежность и высокую скорость при ее передаче по каналам связи (коды: линейные, циклические, БЧХ, Хэмминга, Шеннона - Фано и Хаффмана) Умеет: решать типовые задачи кодирования и декодирования информации с использованием математических методов и моделей Имеет практический опыт: применения помехоустойчивых шифров и кодов, повышающих скорость передачи информации в АСУ
1.Ф.02 Современные киберугрозы в промышленных и корпоративных системах автоматизации	Знает: актуальные угрозы информационной безопасности промышленных компаний, текущее состояние и эволюцию киберугроз как ответную реакцию на внедрение средств и мер информационной безопасности, типы современных киберугроз в промышленных и корпоративных системах автоматизации, актуальные векторы атак на промышленные сети АСУ ТП;средства и меры информационной безопасности, применяемые в промышленных и корпоративных системах автоматизации Умеет: анализировать и оценивать риски информационной безопасности в промышленных и корпоративных системах автоматизации, проводить аналитику современных киберугроз в промышленных и корпоративных системах автоматизации, актуальные векторы атак на промышленные сети АСУ ТП Имеет практический опыт: идентификации и моделирования каналов возможного деструктивного информационно-технического воздействия в промышленных и корпоративных

	системах автоматизации, оценки уязвимостей по отношению к современным киберугрозам промышленных сетей АСУ ТП

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 4 з.е., 144 ч., 82,5 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		11
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)	61,5	61,5
Подготовка к практическим занятиям	45	45
Подготовка текста доклада	16,5	16.5
Консультации и промежуточная аттестация	10,5	10,5
Вид 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	Предварительные сведения из теории графов	16	8	8	0
2	Предварительные сведения из теории случайных процессов	16	8	8	0
3	Математические модели в системах защиты информации	40	20	20	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Понятие графа. Способы задания графа. Виды графов	4
2	1	Оптимизационные задачи на графах.	4
3	2	Понятие случайного процесса. Виды случайных процессов.	4
4	2	Марковские случайные процессы и их параметры.	4
4	3	Понятие угрозы уязвимости. Модели угроз уязвимости.	4
5	3	Теоретико-графовые методы моделирования информационных потоков и систем защиты информации	6
6	3	Аналитические методы нахождения экстремума функций, возникающих при анализе теоретико-графовых моделей	2

7	3	Численные методы нахождения экстремума функций, возникающих при анализе теоретико-графовых моделей	2
8	3	Методы моделирования информационных потоков и систем защиты информации на основе марковских процессов	6

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	1	Понятие графа. Способы задания графа. Виды графов	2
2	1	Оптимизационные задачи на графах.	4
3	1	Контрольная работа "Предварительные сведения из теории графов"	2
4	2	Понятие случайного процесса. Виды случайных процессов. Дискретные и непрерывные случайные процессы	2
5	2	Марковские случайные процессы и их параметры: матрица вероятностей переходов, предельные вероятности.	4
6	2	Контрольная работа "Марковские случайные процессы"	2
7	3	Теоретико-графовые методы моделирования информационных потоков и систем защиты информации. Модель нарушителя и модель системы защиты. Функции, описывающие эффективность атак и характеризующие уровень защищённости.	6
8	3	Аналитические и численные методы нахождения экстремума функций, возникающих при анализе теоретико-графовых моделей: метод Эйлера, волновой метод и др.	6
9	3	Описание теоретико-графовых моделей для конкретных систем защиты информации	2
10	3	Методы моделирования информационных потоков и систем защиты информации на основе марковских процессов	6

5.3. Лабораторные работы

Не предусмотрены

5.4. Самостоятельная работа студента

Выполнение СРС			
Подвид СРС	Список литературы (с указанием разделов, глав, страниц) / ссылка на ресурс	Семестр	Кол-во часов
Подготовка к практическим занятиям	Нестеров, С. А. Основы информационной безопасности : учебник для спо / С. А. Нестеров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 324 с. — ISBN 978-5-8114-9489-7. — Текст : электронный Рацеев, С. М. Математические методы защиты информации : учебное пособие для вузов / С. М. Рацеев. — Санкт-Петербург : Лань, 2022. — 544 с. — ISBN 978-5-8114-8589-5. — Текст : электронный	11	45
Подготовка текста доклада	Нестеров, С. А. Основы информационной безопасности : учебник для спо / С. А.	11	16,5

	Нестеров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 324 с. — ISBN 978-5-8114-9489-7. — Текст : электронный Рацеев, С. М. Математические методы защиты информации : учебное пособие для вузов / С. М. Рацеев. — Санкт-Петербург : Лань, 2022. — 544 с. — ISBN 978-5-8114-8589-5. — Текст : электронный		

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	11	Текущий контроль	Контрольная работа по теме "Предварительные сведения из теории графов"	1	15	15 баллов - задача решена правильно 10-14 баллов -в решение есть неточности и незначительные ошибки 6-9 баллов - общий ход решения верен, но имеются серьёзные недочёты 3-5 баллов - в решении присутствует ряд серьёзных ошибок 1-2 балла - есть некоторый намёк на решение 0 баллов - задача не решалась	экзамен
2	11	Текущий контроль	Контрольная работа по теме "Марковские процессы"	1	15	5 баллов - задача решена правильно 10-14 баллов -в решение есть неточности и незначительные ошибки 6-9 баллов - общий ход решения верен, но имеются серьёзные недочёты 3-5 баллов - в решении присутствует ряд серьёзных ошибок 1-2 балла - есть некоторый намёк на решение 0 баллов - задача не решалась	экзамен
3	11	Текущий контроль	Доклад	1	10	10 баллов - тема доклада полностью раскрыта 7-9 баллов - есть некоторые не полностью раскрытые аспекты темы 4- 6 баллов - есть полностью не раскрытые аспекты темы 1-3 балла - в теме раскрыты лишь	экзамен

						некоторые аспекты 0 баллов - тема не раскрыта	
4	11	Проме-жуточная аттестация	Экзамен	-	40	40 баллов - получен правильный ответ на все вопросы билета 30-39 балла - получен правильный ответ на 3 вопроса билета (возможны мелкие недочёты) 20-29 балла - получен правильный ответ на 1 вопрос билета (имеются серьёзные недочёты) 1-19 баллов - имеются попытки ответить на какие-то вопросы билета 0 баллов - нет попыток ответить на вопросы билета	экзамен

6.2. Процедура проведения, критерии оценивания

Вид промежуточной аттестации	Процедура проведения	Критерии оценивания
экзамен	При оценивании результата мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.19 N 179). На экзамене происходит оценивание учебной деятельности на основе оценок за мероприятия текущего контроля. Студент может улучшить свой рейтинг пройдя мероприятие текущей аттестации.	В соответствии с пп. 2.5, 2.6 Положения

6.3. Паспорт фонда оценочных средств

Компетенции	Результаты обучения	№ КМ			
		1	2	3	4
ПК-1	Знает: основные виды математических моделей информационных потоков и систем защиты информации и методы их построения	+	+	+	+
ПК-1	Умеет: на основе опытных данных и технических характеристик автоматизированной системы управления (АСУ) строить адекватную математическую модель, связанную с системой защиты информации в АСУ		+		+
ПК-1	Имеет практический опыт: применения математических моделей для построения системы защиты информации в АСУ и оценки ее эффективности		+		+

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:

Не предусмотрены

г) методические указания для студентов по освоению дисциплины:

1. Г.И. Радченко "Распределённые вычислительные системы"

из них: учебно-методическое обеспечение самостоятельной работы студента:

1. Г.И. Радченко "Распределённые вычислительные системы"

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
1	Основная литература	Электронно-библиотечная система издательства Лань	Нестеров, С. А. Основы информационной безопасности : учебник для спо / С. А. Нестеров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 324 с. — ISBN 978-5-8114-9489-7. — Текст : электронный https://e.lanbook.com/book/195510
2	Дополнительная литература	Электронно-библиотечная система издательства Лань	Рацеев, С. М. Математические методы защиты информации : учебное пособие для вузов / С. М. Рацеев. — Санкт-Петербург : Лань, 2022. — 544 с. — ISBN 978-5-8114-8589-5. — Текст : электронный https://e.lanbook.com/book/193323

Перечень используемого программного обеспечения:

Нет

Перечень используемых профессиональных баз данных и информационных справочных систем:

Нет

8. Материально-техническое обеспечение дисциплины

Не предусмотрено