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: 29.05.2022

А. Н. Соколов

РАБОЧАЯ ПРОГРАММА

дисциплины 1.О.39.01 Разработка автоматизированных систем в защищенном исполнении
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: 29.05.2022

А. Н. Соколов

Разработчик программы,
старший преподаватель

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Мищенко Е. Ю.
Пользователь: mishchenkoei
Дата подписания: 28.05.2022

Е. Ю. Мищенко

Челябинск

1. Цели и задачи дисциплины

Целью изучения дисциплины является теоретическая и практическая подготовка специалистов к деятельности, связанной с разработкой защищенных автоматизированных информационных систем в своей профессиональной деятельности. Задачи дисциплины: - изучение основных угроз безопасности информации в автоматизированных систе-мах и освоение методик оценки данных угроз; - изучение методов, способов, средств, последовательности и содержания этапов раз-работки автоматизированных систем и подсистем безопасности автоматизирован-ных систем; - изучение основных мер по защите информации в автоматизированных системах; - изучение содержания и порядка деятельности персонала по эксплуатации защищен-ных автоматизированных систем и подсистем безопасности автоматизированных систем. - изучение методов и средств разработки автоматизированных систем и подсистем безопасности автоматизированных систем; - изучение содержания основных этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем; - изучение методов, способов и средств обеспечения отказоустойчивости автоматизированных систем; - изучение основных мер по защите информации в автоматизированных системах; - формирование у обучаемых научного подхода к осмыслению процессов обработки, хранения и передачи информации.

Краткое содержание дисциплины

Защищенные АИС. Основные понятия и классификация. Требования защищенности автоматизированных систем в условиях ак-туальных угроз безопасности информации Определение и содержание понятия угрозы безопасности автоматизированных систем Оценка угроз безопасности автоматизированных систем Стадии и этапы разработки автоматизированных систем Автоматизированное проектирование Разработка автоматизированных систем в защищенном исполнении

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине
ОПК-11 Способен разрабатывать компоненты систем защиты информации автоматизированных систем	Знает: основные меры по защите информации в автоматизированных системах; содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем безопасности автоматизированных систем Умеет: настраивать программное обеспечение системы защиты информации автоматизированной системы Имеет практический опыт: выявления и анализа уязвимостей автоматизированной системы, приводящих к возникновению угроз безопасности информации
ОПК-14 Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите	Знает: критерии оценки защищенности автоматизированной системы; основные угрозы безопасности информации и модели нарушителя

информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений	в автоматизированных системах Умеет: контролировать уровень защищенности в автоматизированных системах Имеет практический опыт: анализа событий, связанных с защитой информации в автоматизированных системах

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
1.О.08 Экономика и управление на предприятии	1.О.39.02 Эксплуатация автоматизированных систем в защищенном исполнении, 1.О.47 Основы аттестации 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.08 Экономика и управление на предприятии	Знает: подходы к классификации факторов внешней среды организации и их влияние на деятельность организации, основы построения, расчета и анализа современной системы показателей, характеризующих деятельность хозяйствующих субъектов на микроуровне Умеет: формулировать управленческие решения по результатам анализа внешней и внутренней среды организации, осуществлять расчет себестоимости продукции; рассчитывать влияние факторов на различные виды расходов; осуществлять расчет потребности в инвестициях Имеет практический опыт: методами оценки экономической эффективности результатов хозяйственной деятельности различных субъектов экономической системы, владения методами распределения накладных затрат и оценки эффективности проектных решений

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 3 з.е., 108 ч., 66,25 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		8
Общая трудоёмкость дисциплины	108	108
Аудиторные занятия:	60	60
Лекции (Л)	24	24

Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	36	36
Лабораторные работы (ЛР)	0	0
Самостоятельная работа (СРС)	41,75	41,75
Самостоятельное изучение теоретического мате-риала	30	30
Выполнение индивидуальных заданий по моду-лю	11,75	11.75
Консультации и промежуточная аттестация	6,25	6,25
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	Требования защищенности автоматизированных систем в условиях ак-туальных угроз безопасности информации	28	10	18	0
2	Разработка защищенных автоматизированных систем	32	14	18	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Критерии оценки защищенности автоматизированных систем. ГОСТ 15408 часть1 общие положения	2
2	1	Оценка угроз безопасности автоматизированных систем. Модель угроз безопасности инфрпмации	4
7	1	Критерии оценки защищенности автоматизированных систем. ГОСТ 15408 часть 2 Функции безопасности	4
3	2	Стадии и этапы разработки автоматизированных систем	2
4	2	Техническое задание на создание автоматизированных систем	4
5	2	Разработка автоматизированных систем в защищенном исполнении	2
6	2	Реализация моделей безопасности автоматизированных систем	2
8	2	автоматизированные системы в защищенном исполнении для объектов КИИ	4

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	1	Модели данных, систем и процессов защиты информации в автоматизированных системах	4
2	1	Критерии оценки защищенности автоматизированных систем	2
3	1	Определение и содержание понятия угрозы безопасности автоматизированных систем	2
4	1	Требования защищенности автоматизированных систем в условиях ак-туальных угроз безопасности информации	2
5	1	Порядок разработки модели угроз и нарушителей информационной безопасности автоматизированных систем	4
6	1	Оценка угроз безопасности информационных систем персональных дан-ных	4
7	2	Стадии и этапы разработки автоматизированных систем	4

8	2	Техническое задание на создание системы защиты информации	4
9	2	Работы на стадиях и этапах создания автоматизированных систем в защищенном исполнении	4
10	2	Ввод в эксплуатацию защищенных автоматизированных систем	2
11	2	Автоматизированные системы в защищенном исполнении для объектов КИИ	4

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
Самостоятельное изучение теоретического мате-риала	Солодянников, А. В. Информационная безопасность автоматизированных систем / А. В. Солодянников. – Санкт-Петербург : Санкт-Петербургский государственный экономический университет, 2020. – 108 с.	8	30
Выполнение индивидуальных заданий по моду-лю	Давидюк, Н. В. Разработка автоматизированных систем обработки информации в защищенном исполнении : учебное пособие / Н. В. Давидюк. — Санкт-Петербург : Интермедия, 2020. — 48 с.	8	11,75

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	Проме-жуточная аттестация	контрольная работа	-	2	полный ответ - 2 балла, неполный ответ - 1 балл, неправильный ответ - 0 баллов	зачет
2	8	Текущий контроль	модель угроз ИСПДн	1	2	0 - не представлено, 1 - сделано с ошибками, 2 - сделано правильно	зачет
3	8	Текущий контроль	модель угроз ГИС	1	2	0 - не представлено, 1 - сделано с ошибками, 2 - сделано правильно	зачет
4	8	Текущий контроль	техническое задание на создание/модернизацию АСЗИ	1	2	0 - не представлено, 1 - сделано с ошибками, 2 - сделано правильно	зачет

6.2. Процедура проведения, критерии оценивания

Вид промежуточной аттестации	Процедура проведения	Критерии оценивания
зачет	Студент получает один вопрос. отвечает устно преподавателю. Полный и неполный ответ - зачет, неправильный ответ - незачет	В соответствии с пп. 2.5, 2.6 Положения

6.3. Паспорт фонда оценочных средств

Компетенции	Результаты обучения	№ КМ			
		1	2	3	4
ОПК-11	Знает: основные меры по защите информации в автоматизированных системах; содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем безопасности автоматизированных систем	+	+	+	+
ОПК-11	Умеет: настраивать программное обеспечение системы защиты информации автоматизированной системы	+			
ОПК-11	Имеет практический опыт: выявления и анализа уязвимостей автоматизированной системы, приводящих к возникновению угроз безопасности информации	+	+	+	+
ОПК-14	Знает: критерии оценки защищенности автоматизированной системы; основные угрозы безопасности информации и модели нарушителя в автоматизированных системах	+	+	+	+
ОПК-14	Умеет: контролировать уровень защищенности в автоматизированных системах	+	+	+	+
ОПК-14	Имеет практический опыт: анализа событий, связанных с защитой информации в автоматизированных системах	+	+	+	+

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. Емельянов Н.З., Партыка Т.Л., Попов И.И. Основы построения автоматизированных информационных систем. Учебное пособие. - М.: ФОРУМ: ИНФРА-М, 2005.

из них: учебно-методическое обеспечение самостоятельной работы студента:

1. Емельянов Н.З., Партыка Т.Л., Попов И.И. Основы построения автоматизированных информационных систем. Учебное пособие. - М.: ФОРУМ: ИНФРА-М, 2005.

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
1	Основная литература	eLIBRARY.RU	Солодянников, А. В. Информационная безопасность автоматизированных систем / А. В. Солодянников. – Санкт-Петербург : Санкт-Петербургский государственный экономический университет, 2020. – 108 с. https://elibrary.ru/item.asp?id=43774446
2	Основная литература	Электронно-библиотечная система издательства Лань	Давидюк, Н. В. Разработка автоматизированных систем обработки информации в защищенном исполнении : учебное пособие / Н. В. Давидюк. — Санкт-Петербург : Интермедия, 2020. — 48 с. https://e.lanbook.com/book/161365
3	Дополнительная литература	eLIBRARY.RU	Алгоритм создания автоматизированных систем в защищенном исполнении / А. М. Каднова, О. Ю. Макаров, С. А. Мишин, Е. А. Рогозин // Безопасность информационных технологий. – 2019. – Т. 26. – № 4. – С. 93-100. https://elibrary.ru/item.asp?id=41528391
4	Дополнительная литература	eLIBRARY.RU	Хисамов, Ф. Г. Математическая модель оценки защищенности информации от несанкционированного доступа при проектировании автоматизированных систем в защищенном исполнении / Ф. Г. Хисамов, А. С. Жук, Р. С. Шерстобитов // Известия ЮФУ. Технические науки. – 2017. – № 9(194). – С. 91-102. https://elibrary.ru/item.asp?id=32398325
5	Дополнительная литература	eLIBRARY.RU	Методики оценивания надежности систем защиты информации от несанкционированного доступа в автоматизированных системах / О. И. Бокова, И. Г. Дровникова, А. С. Етепнев [и др.] // Труды СПИИРАН. – 2019. – Т. 18. – № 6. – С. 1301-1332. https://elibrary.ru/item.asp?id=41478659

Перечень используемого программного обеспечения:

1. Microsoft-Windows(бессрочно)
2. Microsoft-Office(бессрочно)

Перечень используемых профессиональных баз данных и информационных справочных систем:

1. -Консультант Плюс(31.07.2017)

8. 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, Mozila Firefox, Консультант+.
Лабораторные занятия	913 (3б)	Комплект компьютерного оборудования; Локальная вычислительная сеть; Коммутатор, Программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozila Firefox, Консультант+; Локальные СЗИ: Secret Net 6.5 (автономный вариант), Страж 3.0; Межсетевые экраны: ViPNet Custom 3.1, User Gate 5.2
Практические занятия и семинары	913 (3б)	Комплект компьютерного оборудования; Локальная вычислительная сеть; Коммутатор, Программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozila Firefox, Консультант+; Локальные СЗИ: Secret Net 6.5 (автономный вариант), Страж 3.0; Межсетевые экраны: ViPNet Custom 3.1, User Gate 5.2