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: 25.06.2024

А. Н. Соколов

РАБОЧАЯ ПРОГРАММА

дисциплины 1.О.39.02 Эксплуатация 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: 25.06.2024

А. Н. Соколов

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

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: 25.06.2024

А. Н. Соколов

Челябинск

1. Цели и задачи дисциплины

Целью изучения дисциплины является теоретическая и практическая подготовка специалистов к деятельности, связанной с разработкой и эксплуатацией защищенных автоматизированных информационных систем в своей профессиональной деятельности. Задачи дисциплины: - изучение методов, способов и средств обеспечения отказоустойчивости автоматизированных систем; - изучение основных мер по защите информации в автоматизированных системах; - овладение навыками эксплуатации автоматизированных информационных систем для решения различных классов задач; - формирование у обучаемых научного подхода к осмыслению процессов обработки, хранения и передачи информации; - 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.

Краткое содержание дисциплины

Основы эксплуатации защищенных АИС. Диагностика программных и аппаратных средств АИС.

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: основные информационные технологии, используемые в автоматизированных системах; методы, способы и средства обеспечения отказоустойчивости автоматизированных систем Умеет: восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нештатных ситуациях Имеет практический опыт: поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем
ОПК-14 Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений	Знает: организационные, правовые, программно-аппаратные, криптографические, технические меры по защите информации, реализуемые в автоматизированных системах Умеет: администрировать подсистемы информационной безопасности автоматизированных систем Имеет практический опыт: использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин,	Перечень последующих дисциплин,

видов работ учебного плана	видов работ
ФД.02 Мониторинг информационной безопасности и активный поиск киберугроз, 1.О.31 Защита информации от утечки по техническим каналам, 1.О.37 Информационная безопасность открытых систем, 1.О.09 Экономика и управление на предприятии, 1.О.39.01 Разработка автоматизированных систем в защищенном исполнении	Не предусмотрены

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

Дисциплина	Требования
1.О.39.01 Разработка автоматизированных систем в защищенном исполнении	Знает: основные меры по защите информации в автоматизированных системах;содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем безопасности автоматизированных систем, критерии оценки защищенности автоматизированной системы;основные угрозы безопасности информации и модели нарушителя в автоматизированных системах Умеет: настраивать программное обеспечение системы защиты информации автоматизированной системы, контролировать уровень защищенности в автоматизированных системах Имеет практический опыт: выявления и анализа уязвимостей автоматизированной системы, приводящих к возникновению угроз безопасности информации, анализа событий, связанных с защитой информации в автоматизированных системах
1.О.09 Экономика и управление на предприятии	Знает: основы построения, расчета и анализа современной системы показателей, характеризующих деятельность хозяйствующих субъектов на микроуровне, подходы к классификации факторов внешней среды организации и их влияние на деятельность организации Умеет: осуществлять расчет себестоимости продукции; рассчитывать влияние факторов на различные виды расходов; осуществлять расчет потребности в инвестициях, формулировать управленческие решения по результатам анализа внешней и внутренней среды организации Имеет практический опыт: владения методами распределения накладных затрат и оценки эффективности проектных решений, методами оценки экономической эффективности результатов хозяйственной деятельности различных субъектов экономической системы

1.О.37 Информационная безопасность открытых систем	Знает: риски подсистем защиты информации автоматизированных систем и экспериментальные методы их оценки , принципы формирования политики информационной безопасности в автоматизированных системах Умеет: анализировать и оценивать угрозы информационной безопасности автоматизированных систем, разрабатывать частные политики информационной безопасности автоматизированных систем Имеет практический опыт: анализа информационной инфраструктуры автоматизированных систем, управления процессами обеспечения безопасности автоматизированных систем
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
1.О.31 Защита информации от утечки по техническим каналам	Знает: типовые методики проведения измерений параметров, характеризующих наличие технических каналов утечки информации, 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 Умеет: проводить контрольно-измерительные работы в целях оценки количественных характеристик технических каналов утечки информации, использовать средства инструментального контроля показателей эффективности технической защиты информации Имеет практический опыт: проектирования системы защиты объекта информатизации от утечек по техническим каналам

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 3 з.е., 108 ч., 56,5 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		9
Общая трудоёмкость дисциплины	108	108
Аудиторные занятия:	48	48
Лекции (Л)	16	16
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	32	32
Лабораторные работы (ЛР)	0	0
Самостоятельная работа (СРС)	51,5	51,5
Подготовка к практическим занятиям	51,5	51.5
Консультации и промежуточная аттестация	8,5	8,5
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	Основы эксплуатации защищенных АИС	26	8	18	0
2	Диагностика программных и аппаратных средств АИС	22	8	14	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Аттестация АИС по требованиям безопасности. Содержание основных документов, определяющих цели, задачи, порядок проведения аттестации. Требования и рекомендации по защите служебной тайны и персональных данных при работе АИС. Порядок обеспечения защиты информации при эксплуатации АИС	2
2	1	Особенности эксплуатации АИС на объекте защиты. Технические и программные средства защиты АИС от несанкционированного доступа. Организация технического обслуживания защищенных АИС. Содержание и порядок ведения эксплуатационной документации	4
3	1	Методы проверки защищенных АИС. Содержание и порядок ведения эксплуатационной документации	2
4	2	Средства диагностирования защищенных АИС. Контрольно-измерительное оборудование, используемое при поиске неисправностей аппаратных средств	2
5	2	Технологическое оборудование для ремонта аппаратных средств АИС. Диагностические программы и пакеты диагностических программ, их назначение, возможности и порядок использования	2
6	2	Аппаратно-программные средства диагностики АИС	2
7	2	Аппаратно-программные средства контроля функционирования отдельных элементов, узлов, блоков.	2

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	1	Анализ основных документов, определяющих цели, задачи, порядок проведения аттестации	4
2	1	Анализ требований к эксплуатации АИС на объекте защиты	4
3	1	Анализ этапов обеспечения защиты информации при эксплуатации АИС	4
4	1	Содержание и порядок ведения эксплуатационной документации, при организации технического обслуживания защищенных АИС	4
5	1	Анализ содержания и порядка ведения эксплуатационной документации	2
6	2	Контрольно-измерительное оборудование, используемое при поиске неисправностей аппаратных средств	4
7	2	Диагностические программы и пакеты диагностических про-грамм, их назначение, возможности и порядок использова-ния	4
8	2	Аппаратно-программные средства диагностики АИС	4
9	2	Аппаратно-программные средства контроля функционирования отдельных элементов, узлов, блоков	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
Подготовка к практическим занятиям	Вся доступная литература	9	51,5

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	9	Текущий контроль	Контрольная работа 1	1	3	полный ответ - 3 балла, неполный ответ - 1 балл, неправильный ответ - 0 баллов	экзамен
2	9	Текущий контроль	Контрольная 2	1	3	полный ответ - 3 балла, неполный ответ - 1 балл, неправильный ответ - 0 баллов	экзамен
3	9	Проме-жуточная аттестация	Экзамен	-	2	Студент получает два вопроса. отвечает устно преподавателю. Полный ответ на каждый поставленный вопрос даёт балл,	экзамен

						частичный даёт половину балла	

6.2. Процедура проведения, критерии оценивания

Не предусмотрены

6.3. Паспорт фонда оценочных средств

Компетенции	Результаты обучения	№ КМ		
		1	2	3
ОПК-13	Знает: основные информационные технологии, используемые в автоматизированных системах; методы, способы и средства обеспечения отказоустойчивости автоматизированных систем	+		
ОПК-13	Умеет: восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нештатных ситуациях	+		+
ОПК-13	Имеет практический опыт: поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем			+
ОПК-14	Знает: организационные, правовые, программно-аппаратные, криптографические, технические меры по защите информации, реализуемые в автоматизированных системах		+	
ОПК-14	Умеет: администрировать подсистемы информационной безопасности автоматизированных систем		+	+
ОПК-14	Имеет практический опыт: использования программно-аппаратных средств обеспечения информационной безопасности 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:

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:

Электронная учебно-методическая документация

№	Вид	Наименование	Библиографическое описание

	литературы	ресурса в электронной форме	
1	Основная литература	Электронно-библиотечная система издательства Лань	Брюхомицкий, Ю. А. Безопасность информационных технологий : учебное пособие : в 2 частях / Ю. А. Брюхомицкий. — Ростов-на-Дону : ЮФУ, 2020 — Часть 1 — 2020. — 171 с. — ISBN 978-5-9275-3571-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/170337 (дата обращения: 15.11.2021). — Режим доступа: для авториз. пользователей.
2	Основная литература	Электронно-библиотечная система издательства Лань	Аверченков, В. И. Автоматизация проектирования комплексных систем защиты информации : монография / В. И. Аверченков, М. Ю. Рытов, О. М. Голембиовская. — 2-е изд. — Москва : ФЛИНТА, 2017. — 145 с. — ISBN 978-5-9765-2945-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/92913 (дата обращения: 15.11.2021). — Режим доступа: для авториз. пользователей.
3	Основная литература	Электронно-библиотечная система издательства Лань	Беловицкий, К. Б. Коммерческий шпионаж (противодействие) : учебное пособие / К. Б. Беловицкий. — Москва : РТУ МИРЭА, 2021. — 273 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/176522 (дата обращения: 15.11.2021). — Режим доступа: для авториз. пользователей.
4	Дополнительная литература	Образовательная платформа Юрайт	Запечников, С. В. Криптографические методы защиты информации : учебник для вузов / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — Москва : Издательство Юрайт, 2021. — 309 с. — (Высшее образование). — ISBN 978-5-534-02574-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/468902

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
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

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