ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Директор института
Высшая школа электроники и компьютерных наук

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Голлай А. В.
Пользователь: gollaiav
Дата подписания: 15.10.2021

А. В. Голлай

РАБОЧАЯ ПРОГРАММА

дисциплины Б.1.30.01 Разработка защищенных автоматизированных систем
для специальности 10.05.03 Информационная безопасность автоматизированных систем
уровень специалист **тип программы** Специалитет
специализация Информационная безопасность автоматизированных систем критически важных объектов
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 01.12.2016 № 1509

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: 15.10.2021

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: 15.10.2021

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 (ЗУНы)
ПК-2 способностью создавать и исследовать модели автоматизированных систем	Знать:основные угрозы безопасности информации и модели нарушителя в автоматизированных системах
	Уметь:исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений
	Владеть:методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем; навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем
ПК-16 способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом	Знать:методы аттестации уровня защищенности информационных систем
	Уметь:

нормативных документов по защите информации	Владеть:
ПК-6 способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности	Знать:основные информационные технологии, используемые в автоматизированных системах; основные угрозы безопасности информации и модели нарушителя в автоматизированных системах
	Уметь:
	Владеть:навыками анализа основных узлов и устройств современных автоматизированных систем; навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем
ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	Знать:основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические); основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах
	Уметь:
	Владеть:
ПК-13 способностью участвовать в проектировании средств защиты информации автоматизированной системы	Знать:основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности; основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические); основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах
	Уметь:исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений
	Владеть:методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Б.1.28 Безопасность операционных систем,	Б.1.30.02 Эксплуатация защищенных

Б.1.29 Безопасность систем баз данных, Б.1.22 Организация ЭВМ и вычислительных систем	автоматизированных систем

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

Дисциплина	Требования
Б.1.28 Безопасность операционных систем	Знание основных видов и классов операционных систем, методологических и практических подходов к обеспечению безопасности ОС, основных программно-аппаратные средств защиты информации в ОС. Умение использовать на практике базовые средства безопасности ОС различных классов. Навыки установки и настройки операционных систем семейств Windows и Unix с учетом требований по обеспечению информационной безопасности
Б.1.29 Безопасность систем баз данных	Знание основных систем управления баз данных, методов, средств и технологий обеспечения безопасности БД. Умение осуществлять выбор наиболее эффективных средств обеспечения безопасности БД.
Б.1.22 Организация ЭВМ и вычислительных систем	Знание структуры, состава и принципов работы ЭВМ и вычислительных систем. Умение определять необходимую, достаточную и эффективную структуру вычислительной системы

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 3 з.е., 108 ч.

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		8
Общая трудоёмкость дисциплины	108	108
Аудиторные занятия:	48	48
Лекции (Л)	16	16
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	0	0
Лабораторные работы (ЛР)	32	32
Самостоятельная работа (СРС)	60	60
Самостоятельное изучение теоретического мате-риала	30	30
Выполнение индивидуальных заданий по моду-лю	30	30
Вид итогового 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	18	6	0	12
2	Разработка защищенных автоматизированных систем	30	10	0	20

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Критерии оценки защищенности автоматизированных систем	2
2	1	Определение и содержание понятия угрозы безопасности автоматизированных систем	2
3	1	Оценка угроз безопасности автоматизированных систем	2
4	2	Стадии и этапы разработки автоматизированных систем	2
5	2	Автоматизированное проектирование	2
6	2	Разработка автоматизированных систем в защищенном исполнении	2
7	2	Реализация моделей безопасности автоматизированных систем	2
8	2	Особенности разработки информационных систем персональных данных	2

5.2. Практические занятия, семинары

Не предусмотрены

5.3. Лабораторные работы

№ занятия	№ раздела	Наименование или краткое содержание лабораторной работы	Кол-во часов
1	1	Модели данных, систем и процессов защиты информации в автоматизированных системах	4
2	1	Критерии оценки защищенности автоматизированных систем	4
3	1	Определение и содержание понятия угрозы безопасности автоматизированных систем	4
4	2	Порядок разработки модели угроз и нарушителей информационной безопасности автоматизированных систем	4
5	2	Оценка угроз безопасности информационных систем персональных дан-ных	4
6	2	Стадии и этапы разработки автоматизированных систем	4
7	2	Автоматизированные системы проектирования средств и подсистем безопасности	4
8	2	Работы на стадиях и этапах создания автоматизированных систем в защищенном исполнении	4

5.4. Самостоятельная работа студента

Выполнение СРС		
Вид работы и содержание задания	Список литературы (с указанием разделов, глав, страниц)	Кол-во часов
Выполнение индивидуальных заданий по	Основная литература - 1. Доп. литература	30

моду-лю	- 1	
Самостоятельное изучение теоретического мате-риала	Основная литература - 1	30

6. Инновационные образовательные технологии, используемые в учебном процессе

Инновационные формы учебных занятий	Вид работы (Л, ПЗ, ЛР)	Краткое описание	Кол-во ауд. часов
Проектная деятельность	Лабораторные занятия	Индивидуальное задание представляет собой модель автоматизированной (информаци-онной) системы в защищенном исполнении. Разработка модели основывается на устанавли-ваемых, в соответствии с вариантом, требованиях по безопасности информации. Требования устанавливаются относительно класса защиты автоматизированной системы от несанкцио-нированного доступа, уровня защищенности персональных данных, особенностей автомати-зированной системы, а также угроз безопасности информации, характерных для данной сис-темы. Последовательность разработки модели осуществляется поэтапно, в соответствии с последовательностью изучаемых разделов учебной дисциплины. Разработка модели осуще-ствляется в соответствии с требованиями стандарта по созданию систем в защищенном ис-полнении	30

Собственные инновационные способы и методы, используемые в образовательном процессе

Не предусмотрены

Использование результатов научных исследований, проводимых университетом, в рамках данной дисциплины: нет

7. Фонд оценочных средств (ФОС) для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

7.1. Паспорт фонда оценочных средств

Наименование разделов дисциплины	Контролируемая компетенция ЗУНы	Вид контроля (включая текущий)	№№ заданий
Требования защищенности автоматизированных систем в условиях ак-туальных угроз безопасности информации	ПК-13 способностью участвовать в проектировании средств защиты информации автоматизированной системы	Зачет	1-10
Разработка защищенных автоматизированных систем	ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	контрольная работа	1-10
Требования защищенности	ПК-16 способностью участвовать в	Зачет	11-18

автоматизированных систем в условиях ак-туальных угроз безопасности информации	проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации		
Разработка защищенных автоматизированных систем	ПК-2 способностью создавать и исследовать модели автоматизированных систем	Зачет	19-99
Разработка защищенных автоматизированных систем	ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	Зачет	19-99
Разработка защищенных автоматизированных систем	ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	контрольная работа	11-32
Разработка защищенных автоматизированных систем	ПК-6 способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности	контрольная работа	11-32
Разработка защищенных автоматизированных систем	ПК-6 способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности	Зачет	19-99

7.2. Виды контроля, процедуры проведения, критерии оценивания

Вид контроля	Процедуры проведения и оценивания	Критерии оценивания
Зачет	студенты в аудитории письменно отвечают на вопросы зачетного задания, которое включает теоретические вопросы и задачи по пройденным разделам, преподаватель проверяет, беседует и оценивает	Зачтено: Обладает твёрдым и полным знанием материала дисциплины, владеет дополнительными знаниями, даны полные, развёрнутые ответы; логически, грамотно и точно излагает материал дисциплины, интерпретируя его самостоятельно, способен самостоятельно его анализировать и делать выводы. Знает материал дисциплины в запланированном объёме, некоторые моменты в ответе не отражены или в ответе имеются несущественные неточности; грамотно и по существу излагает материал. Не зачтено: Не знает значительной части материала дисциплины; ответ не дан или допускает грубые ошибки при изложении ответа на вопрос; неверно излагает и интерпретирует знания; изложение материала логически не выстроено.
контрольная работа	Преподаватель проверяет и оценивает выполнение самостоятельной работы, студент отвечает на вопросы преподавателя по теоретической и практической части самостоятельной работы	Отлично: обладает твёрдым и полным знанием материала дисциплины, владеет дополнительными знаниями, даны полные, развёрнутые ответы; логически, грамотно и точно излагает материал дисциплины, интерпретируя его самостоятельно, способен самостоятельно его анализировать и делать выводы.

		Хорошо: знает материал дисциплины в запланированном объёме, некоторые моменты в ответе не отражены или в ответе имеются несущественные неточности; грамотно и по существу излагает материал. Удовлетворительно: знает только основной материал дисциплины, не усвоил его деталей, дана только часть ответа на вопросы; в ответе имеются существенные ошибки; допускает неточности в изложении и интерпретации знаний; имеются нарушения логической последовательности в изложении материала. Неудовлетворительно: не знает значительной части материала дисциплины; ответ не дан или допускает грубые ошибки при изложении ответа на вопрос; неверно излагает и интерпретирует знания; изложение материала логически не выстроено.

7.3. Типовые контрольные задания

Вид контроля	Типовые контрольные задания
Зачет	1. Понятие сложной системы. 2. Элементы подсистемы. 3. Управление и информация. 4. Случайнее факторы 5. Самоорганизация 6. Понятие качества и эффективности сложных систем. 7. Эффективность. 8. Надежность. 9. Помехозащищенность. 10. Устойчивость. 11. Сложность. 12. Порядок разработки сложной системы. 13. Этапы разработки. 14. Системотехника. 15. Обоснование технического задания. 16. Что такое информационная система? 17. Классификация информационных систем. 18. Разработка и производство информационных систем. 19. Структура информационной системы и принципы ее функционирования. 20. Принципы построения системы защиты информации. 21. Типовые компоненты информационной системы. 22. Проблемы защиты информационной системы. 23. Проблемы защиты открытых систем клиент/сервер. 24. Защита для открытых информационных систем. 25. Структура и задачи органов, осуществляющих защиту информации. 26. Определение информационных и технических ресурсов, подлежащих защите. 27. Оценка угроз и рисков. 28. Политика информационной безопасности, принципы и виды политики безопасности. 29. Организационно-технические мероприятия. 30. Организация секретного делопроизводства. 31. Организация мероприятий по защите информации. 32. Внедрение и использование средств защиты в автоматизированной системе. 33. Принятие административных решений по уровням обеспечения защиты

	информации. 34. Порядок выполнения работ по защите информации. 35. Этапы выполнения работ по созданию и внедрению средств защиты информации. 36. Программно-технические методы и средства защиты информации. 37. Службы и механизмы защиты. 38. Управление доступом 39. Контроль за работой пользователей. 40. Управление доступом к рабочим места. 41. Регламентация парольного доступа. 42. Защита целостности программ. 43. Управление системой защиты информации. 44. Принципы организации и контроля системы защиты. 45. Реализация политики безопасности. 46. Управление защитой в распределенных сетях. 47. Методы разработки защищенных информационных систем. 48. Модели управления доступом. 49. Проблемы внедрения систем управления доступом. 50. Основные понятия секретной информации. 51. Порядок отнесения информации к государственной тайне. 52. Защита государственной тайны. 53. Сведения, составляющие коммерческую тайну. 54. Определение степени секретности информации. 55. Оценка уязвимости и рисков. 56. Анализ рисков. 57. Разработка методологии оценки. 58. Этапы оценки. 59. Определение и анализ угроз. 60. Требования к системам защиты информации. 61. Организационные требования. 62. Требования к техническому обеспечению. 63. Требования к программному обеспечению. 64. Выбор средств защиты. 65. Модель информационной системы как объекта защиты. 66. Механизмы обеспечения безопасности. (перечислить и рассмотреть один из механизмов.) 67. Внедрение и использование выбранных мер защиты. 68. Основные решения по обеспечению защиты безопасности. 69. Содержание и последовательность работ по защите информации. 70. Построение системы защиты информации. (перечислить этапы и рассмотреть один из этапов) 71. Порядок проведения работ по защите информации. 72. Этапы выполнения работ по созданию средств защиты информации. (перечислить этапы и рассмотреть один из этапов) 73. Реализация организационных и технических мер защиты. 74. Приемка, определение полноты и качества. 75. Контроль целостности средств защиты информации. 76. Сертификация продукции. 77. Процесс сертификации. 78. Сертификация программного обеспечения на соответствие требованиям безопасности. 79. Общие сведения об устройстве биологического нейрона и нервной системы человека. 80. Общий вид базового элемента искусственных нейронных сетей (формального нейрона). 81. Режимы функционирования искусственных нейронных сетей.

	82. Классификация искусственных нейронных сетей по структуре связей, примеры соответствующих НС. 83. Динамические и статические искусственные нейронные сети, примеры соответствующих НС. 84. Классификация искусственных нейронных сетей по способам обучения, примеры соответствующих НС. 85. Коннекционизм. Правило Хебба. 86. Сеть Хопфилда: принципы работы. 87. Сеть Хопфилда с синхронной динамикой. Предельное состояние. 88. Сеть Хопфилда с асинхронной динамикой. Предельное состояние. 89. Обучение сети Хопфилда для решения задачи классификации. 90. Сеть Кохонена: принципы работы. 91. Сеть Кохонена: способ обучения. 92. Нейронные сети с радиально-базисными функциями активации: принцип работы, способ обучения. 93. Персептрон: принцип работы, способ обучения. 94. Статические многослойные нейронные сети: принцип работы. Функции активации. Задача построения аппроксимации отображения по примерам. 95. Аппроксимационные свойства многослойных НС. 96. Обучение многослойных нейронных сетей, как оптимизация. Особенности данной оптимизационной задачи. 97. Быстрое дифференцирование сложной функции. 98. Использование метода обратного распространения ошибок для вычисления градиента оценочной функции по параметрам сети. 99. Использование метода наискорейшего спуска при обучении многослойных НС.
контрольная работа	1. Понятие, виды и структура автоматизированных систем 2. Безопасность АС, ее составляющие. Основные способы и механизмы обеспечения безопасности информации в АС 3. Классификация, идентификация (инвентаризация, каталогизация) и оценивание (категорирование) объектов защиты в АС 4. Классификация (каталогизация), идентификация, спецификация и оценивание угроз безопасности в АС 5. Человеческий фактор в угрозах безопасности. Модель нарушителя безопасности информации в АС (РД Гостехкомиссии) 6. Декомпозиция назначения, целей и задач функционирования АС. Функциональная структура АС и функциональные требования к защищенным СВТ, АС, продуктам и системам ИТ 7. Система и структура функциональных требований по защите от НСД к информации в СВТ (по РД Гостехкомиссии), классы защищенности СВТ 8. Система и структура функциональных требований по защите от НСД в АС (по РД Гостехкомиссии), группы и классы защищенности АС 9. Общая структура требований безопасности к изделиям и системам ИТ, классы функциональных требований безопасности (по ГОСТ Р ИСО/МЭК 15408-2002. Ч.2) 10. Услуги (сервисы) безопасности при взаимодействии открытых систем и механизмы безопасности, их реализующие (по ГОСТ Р ИСО 7498-1-99), взаимоотношение между услугами защиты и уровнями взаимодействия по 7-ми уровневой эталонной модели ВОС 11. Жизненный цикл, стадии создания и содержание работ по созданию АС, особенности создания АС в защищенном исполнении (по ГОСТ 34.601-90, ГОСТ Р 51583) 12. Техническое задание на создание АС, требования по структуре, содержанию, порядку разработки, оформления, согласования и утверждения (по ГОСТ 34.602-89) 13. Особенности Технического задания на создание АС в защищенном исполнении. Составляющие общих требований к АСЗИ и структуру функциональных требований (по

	ГОСТ Р 51624) 14. Жизненный цикл изделий (продуктов и систем) ИТ, общая схема и последовательность создания изделий ИТ 15. Классификация изделий ИТ и функциональные пакеты требований безопасности. Классы защищенности изделий ИТ и пакеты требований доверия безопасности (по ГОСТ Р ИСО/МЭК 15408-2002 и РД Гостехкомиссии) 16. Структура, порядок разработки, регистрации и опубликования профилей защиты для изделий ИТ (по ГОСТ Р ИСО/МЭК 15408-2002 и РД Гостехкомиссии) 17. Структура, назначение и порядок разработки задания по безопасности при создании изделий ИТ, соотношение между профилем защиты и заданием по безопасности. Техническое задание на создание системы ИТ (по ГОСТ Р ИСО/МЭК 15408-2002 и РД Гостехкомиссии) 18. Содержание процесса разработки и ввода в действие изделий (систем) ИТ. Уровни представления проектных решений 19. Проектирование АС как особый вид деятельности, объекты проектирования при создании АС (по РД 50-680-88) 20. Методология (методы и средства) проектирования АС 21. Каноническое (индивидуальное) проектирование АС. Технологическая схема этапов технического и рабочего проектирования 22. Типовое проектирование АС и его методы. Технологическая схема проектирования 23. Управление процессом проектирования АС, его компоненты и специфика 24. Организационная структура, схемы организации работ при проектировании АС и организационные формы проектного коллектива 25. Содержание и специфика управленческого цикла при проектировании АС 26. Методы планирования и управления проектами. Диаграммы Гантта, сетевые графики проектов 27. Автоматизированные системы управления проектами 28. Общие положения по эксплуатации изделий, комплексов, средств деятельности. Составляющие организационных и технических мероприятий по эксплуатации 29. Особенности эксплуатации КС (АС) и защищенных КС (АС в защищенном исполнении). Администрирование КС (АС) 30. Органы управления и планирования эксплуатации защищенных АС 31. Эксплуатационная документация на АС (изделия ИТ). Руководства пользователя и администратора 32. Конструкторские эксплуатационные документы на ТСО и ПО, эксплуатационные документы предприятия

8. Учебно-методическое и информационное обеспечение дисциплины

Печатная учебно-методическая документация

а) основная литература:

1. Галатенко, В. А. Основы информационной безопасности Курс лекций: Учеб. пособие для вузов по специальностям в обл. информ. технологий В. А. Галатенко; Под ред. В. Б. Бетелина; Интернет-ун-т информ. технологий. - 3-е изд. - М.: Интернет-Университет Информационных Технологий, 2006. - 205 с.

б) дополнительная литература:

1. Зегжда, Д. П. Основы безопасности информационных систем [Текст] учеб. пособие для вузов по специальностям "Компьютер. безопасность" и "Комплекс. обеспечение информ. безопасности автоматизир. систем" Д. П. Зегжда, А. М. Ивашко. - М.: Горячая линия - Телеком, 2000. - 449, [2] с. ил.

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

9. Информационные технологии, используемые при осуществлении образовательного процесса

Перечень используемого программного обеспечения:

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

Перечень используемых информационных справочных систем:

1. -Консультант Плюс(31.07.2017)

10. 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