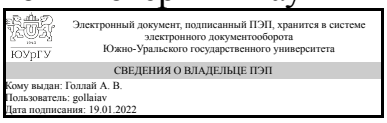
ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Директор института
Высшая школа электроники и компьютерных наук



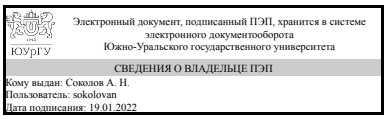
А. В. Голлай

РАБОЧАЯ ПРОГРАММА

дисциплины Б.1.30.02 Эксплуатация 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

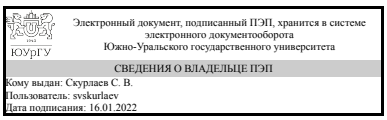
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем, утверждённым приказом Минобрнауки от 01.12.2016 № 1509

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



А. Н. Соколов

Разработчик программы,
старший преподаватель



С. В. Скурлаев

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 (ЗУНы)
ПК-24 способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	Знать:основные информационные технологии, используемые в автоматизированных системах
	Уметь:восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нештатных ситуациях
	Владеть:навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках; навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем; навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем
ОПК-6 способностью применять нормативные правовые акты в профессиональной деятельности	Знать:методы, способы и средства обеспечения отказоустойчивости автоматизированных систем
	Уметь:администрировать подсистемы информационной безопасности автоматизированных систем
	Владеть:навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках; навыками использования программно-аппаратных средств обеспечения

	информационной безопасности автоматизированных систем
ПК-26 способностью администрировать подсистему информационной безопасности автоматизированной системы	Знать:основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем; 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:администрировать подсистемы информационной безопасности автоматизированных систем
	Владеть:
ПК-14 способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	Знать:основные информационные технологии, используемые в автоматизированных системах
	Уметь:
	Владеть:навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем
ПК-18 способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности	Знать:содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем
	Уметь:администрировать подсистемы информационной безопасности автоматизированных систем
	Владеть:

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Б.1.30.01 Разработка защищенных автоматизированных систем	Б.1.43 Аудит информационной безопасности, Производственная практика, преддипломная практика (10 семестр)

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

Дисциплина	Требования
Б.1.30.01 Разработка защищенных автоматизированных систем	Знать: основные информационные технологии, используемые в автоматизированных системах; основные угрозы безопасности информации и

	модели нарушителя в автоматизированных системах; методы аттестации уровня защищенности информационных систем. Владеть: навыками анализа основных узлов и устройств современных автоматизированных систем. Уметь: исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений. Владеть: навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 5 з.е., 180 ч.

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		9
Общая трудоёмкость дисциплины	180	180
Аудиторные занятия:	80	80
Лекции (Л)	32	32
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	32	32
Лабораторные работы (ЛР)	16	16
Самостоятельная работа (СРС)	100	100
Подготовка к практическим занятиям	50	50
Подготовка к лабораторным работам и оформление отчетов	50	50
Вид итогового 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	42	18	18	6
2	Диагностика программных и аппаратных средств АИС	38	14	14	10

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	4
2	1	Особенности эксплуатации АИС на объекте защиты	4
3	1	Требования и рекомендации по защите служебной тайны и персональных	4

		данных при работе АИС. Порядок обеспечения защиты информации при эксплуатации АИС	
4	1	Технические и программные средства защиты АИС от несанкционированного доступа. Организация технического обслуживания защищенных АИС. Содержание и порядок ведения эксплуатационной документации	4
5	1	Методы проверки защищенных АИС. Содержание и порядок ведения эксплуатационной документации	2
6	2	Средства диагностирования защищенных АИС. Контрольно-измерительное оборудование, используемое при поиске неисправностей аппаратных средств	4
7	2	Технологическое оборудование для ремонта аппаратных средств АИС. Диагностические программы и пакеты диагностических программ, их назначение, возможности и порядок использования	4
8	2	Аппаратно-программные средства диагностики АИС	4
9	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

№ занятия	№ раздела	Наименование или краткое содержание лабораторной работы	Кол-во часов
1	1	Изучение программных средства защиты АИС от несанкционированного доступа	6
2	2	Изучение аппаратно-программных средств диагностики АИС	6
3	2	Изучение аппаратно-программных средств контроля функционирования элементов АИС	4

5.4. Самостоятельная работа студента

Выполнение СРС		
Вид работы и содержание задания	Список литературы (с указанием	Кол-во часов

	разделов, глав, страниц)	
Подготовка к лабораторным работам и оформление отчетов	Литература по разделу 8 рабочей программы	50
Подготовка к практическим занятиям	Литература по разделу 8 рабочей программы	50

6. Инновационные образовательные технологии, используемые в учебном процессе

Инновационные формы учебных занятий	Вид работы (Л, ПЗ, ЛР)	Краткое описание	Кол-во ауд. часов
Проектное моделирование	Лабораторные занятия	Моделирование информационной среды, инфраструктуры и автоматизированной системы предприятия для проведения лабораторных работ (на основе локальной сети кафедры)	16

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
Основы эксплуатации защищенных АИС	ОПК-6 способностью применять нормативные правовые акты в профессиональной деятельности	Экзамен	1-5
Основы эксплуатации защищенных АИС	ПК-18 способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности	Экзамен	6-9
Диагностика программных и аппаратных средств АИС	ПК-14 способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	Экзамен	10-15,28
Диагностика программных и аппаратных средств АИС	ПК-24 способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	Экзамен	10-30
Диагностика программных и аппаратных средств АИС	ПК-26 способностью администрировать подсистему информационной безопасности автоматизированной системы	Экзамен	10-30

7.2. Виды контроля, процедуры проведения, критерии оценивания

Вид контроля	Процедуры проведения и оценивания	Критерии оценивания
Экзамен	студенты в аудитории письменно отвечают на вопросы экзаменационного билета, который включает теоретические вопросы и задачи по пройденным разделам, преподаватель проверяет, беседует и оценивает	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
Экзамен	1. Основные понятия и определения. Понятие автоматизированной системы. 2. Особенности автоматизированных систем в защищенном исполнении. 3. Основные виды АС в защищенном исполнении. 4. Основные информационные технологии, используемые в автоматизированных системах. 5. Руководящие документы Гостехкомиссии России (ФСТЭК России). 6. Понятие модели угроз. Документы ФСТЭК России, регламентирующие порядок разработки моделей угроз в автоматизированных системах. Практические подходы к разработке моделей угроз. 7. Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах. 8. Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем. 9. Основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические). 10. Основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах. 11. Порядок администрирования подсистемы информационной безопасности автоматизированных систем. 12. Порядок восстановления работоспособности подсистемы информационной

	безопасности автоматизированных систем в нештатных ситуациях. 13. Этапы разработки технического задания на создание подсистем информационной безопасности автоматизированных систем, проектирование такой подсистемы с учетом действующих нормативных и методических документов. 14. Проектирование защищенных АИС. Методы проектирования. Содержание этапов проектирования. 15. Структура и содержание технического задания на разработку ЗАС. 16. Аттестация АС по требованиям безопасности. Содержание основных документов, определяющих цели, задачи, порядок проведения аттестации. 17. Понятие персональных данных. Понятие ИСПДн. 18. Требования к ИСПДн. Классификация АС. Обезличивание персональных данных. 19. Федеральное законодательство в области защиты персональных данных и ведомственные нормативные акты (ФСТЭК России, ФСБ России) 20. Особенности эксплуатации АС на объекте защиты. Требования и рекомендации по защите персональных данных при работе АС. 21. Особенности эксплуатации АС на объекте защиты. Требования и рекомендации по защите банковской тайны при работе АС. 22. Особенности эксплуатации АС на объекте защиты. Требования и рекомендации по защите коммерческой тайны при работе АС. 23. Порядок обеспечения защиты информации при эксплуатации АС. 24. Технические и программные средства защиты АС от несанкционированного доступа. 25. Организация технического обслуживания защищенных АС. 26. Содержание и порядок ведения эксплуатационной документации. 27. Методы проверки защищенных АС. 28. Средства диагностирования защищенных АС. Контрольно-измерительное оборудование, используемое при поиске неисправностей аппаратных средств АС. 29. Вывод ЗАС из эксплуатации. Порядок организации мероприятий по выводу ЗАС из эксплуатации. 30. Вывод ЗАС из эксплуатации. Содержание организационно-распорядительной документации по выводу ЗАС из эксплуатации.

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:

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
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

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
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
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+.