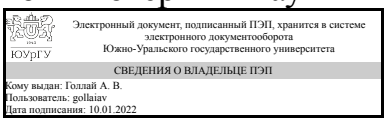
ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Директор института
Высшая школа электроники и компьютерных наук



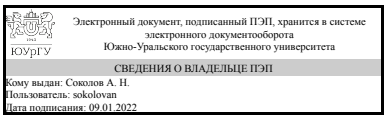
А. В. Голлай

РАБОЧАЯ ПРОГРАММА

дисциплины Б.1.37 Комплексное обеспечение защиты информации объекта информатизации
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

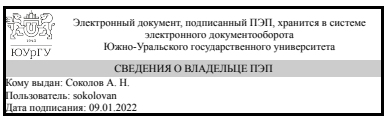
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем, утверждённым приказом Минобрнауки от 01.12.2016 № 1509

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



А. Н. Соколов

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



А. Н. Соколов

Челябинск

1. Цели и задачи дисциплины

Целью изучения дисциплины является теоретическая и практическая подготовка специалистов к деятельности, связанной с комплексным анализом возможных угроз и созданием адекватной модели нарушителя, постановкой конкретных задач заданной степени сложности в рамках модели для обеспечения информационной безопасности автоматизированных систем, а также содействие фундаментализации образования и развитию системного мышления. Задачи дисциплины: - изучение основных аспектов обеспечения информационной безопасности государства; - изучение методологии создания систем защиты информации; - изучение процессов сбора, передачи и накопления информации; - изучение основных элементов теории компьютерной безопасности; - изучение математических основ моделей безопасности; - изучение вопросов оценки защищенности и обеспечения безопасности компьютерных систем.

Краткое содержание дисциплины

Понятие национальной безопасности Российской Федерации. Роль и место информационной безопасности в системе национальной безопасности. Основы государственной политики Российской Федерации в области информационной безопасности. Информационное противоборство и способы его осуществления. Методы и средства обеспечения безопасности объектов информационной инфраструктуры Российской Федерации.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине (ЗУНы)
ПК-5 способностью проводить анализ рисков информационной безопасности автоматизированной системы	Знать:Принципы формирования комплекса мер по обеспечению информационной безопасности предприятия (организации)
	Уметь:Определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем
	Владеть:Навыками анализа информационной инфраструктуры информационной системы и ее безопасности
ПК-22 способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	Знать:Основные принципы формирования комплекса мер по обеспечению информационной безопасности предприятия (организации)
	Уметь:Определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем
	Владеть:Методами выявления угроз информационной безопасности информационных систем

	Знать:Принципы формирования комплекса мер по обеспечению информационной безопасности предприятия (организации)
ПК-23 способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	Уметь:Определять комплекс мер для обеспечения информационной безопасности информационных систем
	Владеть:Методами аудита угроз информационной безопасности информационных систем
ПК-26 способностью администрировать подсистему информационной безопасности автоматизированной системы	Знать:Принципы формирования комплекса мер по обеспечению информационной безопасности предприятия (организации)
	Уметь:Проводить мониторинг угроз безопасности информационных систем
	Владеть:Методами мониторинга угроз информационной безопасности информационных систем

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Б.1.24.01 Организационное обеспечение информационной безопасности, Б.1.21 Программно-аппаратные средства обеспечения информационной безопасности	ДВ.1.06.01 Защита электронного документооборота

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

Дисциплина	Требования
Б.1.21 Программно-аппаратные средства обеспечения информационной безопасности	Знания: принципы работы и организацию современных средств защиты информации; Умения: администрировать средства защиты информации; Навыки: выбор средств защиты информации.
Б.1.24.01 Организационное обеспечение информационной безопасности	Знания: основные руководящие документы, регламентирующие защиту информации на объекте информатизации; Умения: определить рациональные меры по обеспечению организационной защиты на объекте; Навыки: разработки проектов нормативных и правовых актов предприятия, регламентирующих деятельность по обеспечению информационной безопасности.

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 4 з.е., 144 ч.

Вид учебной работы	Всего	Распределение по семестрам

	часов	в часах
		Номер семестра
		8
Общая трудоёмкость дисциплины	144	144
Аудиторные занятия:	64	64
Лекции (Л)	32	32
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	32	32
Лабораторные работы (ЛР)	0	0
Самостоятельная работа (СРС)	80	80
Курсовая работа	80	80
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	Информационная безопасность в системе национальной безопасности Российской Федерации	8	4	4	0
2	Основы государственной политики Российской Федерации в области информационной безопасности	20	10	10	0
3	Информационное противоборство, методы и средства его осуществления	8	4	4	0
4	Методы и средства обеспечения информационной безопасности объектов информационной инфраструктуры	28	14	14	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Понятие национальной безопасности Российской Федерации. Национальные интересы и угрозы национальной безопасности.	2
2	1	Роль и место информационной безопасности в системе национальной безопасности Российской Федерации.	2
3	2	Национальные интересы Российской Федерации в информационной сфере.	2
4	2	Виды и источники угроз информационной безопасности Российской Федерации.	2
5	2	Конституция Российской Федерации о правах и свободах человека и гражданина в информационной сфере. Виды защищаемой информации.	2
6	2	Организационная система обеспечения информационной безопасности Российской Федерации.	2
7	2	Структура законодательства Российской Федерации в информационной сфере. Уголовно-процессуальная характеристика компьютерных преступлений.	2
8	3	Понятие информационного противоборства. Информационные войны, методы и средства их ведения.	2
9	3	Информационное оружие, его классификация и возможности.	2
10	4	Стратегические цели и основные направления, принципы и общие методы обеспечения информационной безопасности.	2

11	4	Автоматизированная информационная система как объект защиты.	2
12	4	Понятие комплексного обеспечения информационной безопасности.	2
13	4	Модели и стратегии обеспечения информационной безопасности автоматизированных информационных систем.	2
14	4	Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.	2
15	4	Общая характеристика методов и средств защиты информации в автоматизированных информационных системах	2
16	4	Задачи и организационная структура подразделения обеспечения информационной безопасности.	2

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	1	Понятие национальной безопасности Российской Федерации. Национальные интересы и угрозы национальной безопасности.	2
2	1	Роль и место информационной безопасности в системе национальной безопасности Российской Федерации.	2
3	2	Национальные интересы Российской Федерации в информационной сфере.	2
4	2	Виды и источники угроз информационной безопасности Российской Федерации.	2
5	2	Конституция Российской Федерации о правах и свободах человека и гражданина в информационной сфере. Виды защищаемой информации.	2
6	2	Система обеспечения информационной безопасности Российской Федерации.	2
7	2	Структура законодательства Российской Федерации в информационной сфере. Уголовно-процессуальная характеристика компьютерных преступлений.	2
8	3	Понятие информационного противоборства. Информационные войны, методы и средства их ведения.	2
9	3	Информационное оружие, его классификация и возможности.	2
10	4	Стратегические цели и основные направления, принципы и общие методы обеспечения информационной безопасности.	2
11	4	Автоматизированная информационная система как объект защиты.	2
12	4	Понятие комплексного обеспечения информационной безопасности.	2
13	4	Модели и стратегии обеспечения информационной безопасности автоматизированных информационных систем.	2
14	4	Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.	2
15	4	Общая характеристика методов и средств защиты информации в автоматизированных информационных системах	2
16	4	Задачи и организационная структура подразделения обеспечения информационной безопасности.	2

5.3. Лабораторные работы

Не предусмотрены

5.4. Самостоятельная работа студента

Выполнение СРС		
Вид работы и содержание задания	Список литературы (с указанием разделов, глав, страниц)	Кол-во часов
Курсовая работа	Основные и дополнительные источники	48
Проработка лекционного материала	Основные источники	32

6. Инновационные образовательные технологии, используемые в учебном процессе

Инновационные формы учебных занятий	Вид работы (Л, ПЗ, ЛР)	Краткое описание	Кол-во ауд. часов
Использование методик оценки уязвимостей субъектов защиты информации	Практические занятия и семинары	Использование методик оценки уязвимостей субъектов защиты информации	2

Собственные инновационные способы и методы, используемые в образовательном процессе

Инновационные формы обучения	Краткое описание и примеры использования в темах и разделах
Набор кейсов	Междисциплинарный практический компонент по работе с кейсами «Управление проектами по защите информации»

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

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
Все разделы	ПК-5 способностью проводить анализ рисков информационной безопасности автоматизированной системы	Контрольные вопросы и задания для проведения текущего и итогового контроля	1-8
Все разделы	ПК-22 способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	Контрольные вопросы и задания для проведения текущего и итогового контроля	9-15
Все разделы	ПК-23 способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	Контрольные вопросы и задания для проведения текущего и итогового контроля	16-25
Все разделы	ПК-26 способностью администрировать подсистему информационной безопасности автоматизированной системы	Контрольные вопросы и задания для проведения текущего и итогового контроля	26-30

7.2. Виды контроля, процедуры проведения, критерии оценивания

Вид контроля	Процедуры проведения и оценивания	Критерии оценивания
Контрольные вопросы и задания для проведения текущего и итогового контроля	Тестирование	Отлично: Оценка «отлично» выставляется за 25 и более правильных ответов на вопросы теста Хорошо: Оценка «хорошо» выставляется за 20-24 правильных ответов на вопросы теста Удовлетворительно: Оценка «удовлетворительно» выставляется за 15-19 правильных ответов на вопросы теста Неудовлетворительно: Оценка «неудовлетворительно» выставляется за 14 и менее правильных ответов на вопросы теста

7.3. Типовые контрольные задания

Вид контроля	Типовые контрольные задания
Контрольные вопросы и задания для проведения текущего и итогового контроля	Тест_ЗИ.docx

8. 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:

1. Безопасность информационных технологий 12+ М-во образования и науки Рос. Федерации, Моск. инж.-физ. ин-т (гос. ун-т), ВНИИПВТИ журнал. - М., 1997-
2. Вестник УрФО : Безопасность в информационной сфере Юж.-Урал. гос. ун-т; ЮУрГУ журнал. - Челябинск: Издательство ЮУрГУ, 2011-

г) методические указания для студентов по освоению дисциплины:

1. Перечень ГОСТов

из них: учебно-методическое обеспечение самостоятельной работы студента:

1. Перечень ГОСТов

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание

1	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: 09.01.2022). — Режим доступа: для авториз. пользователей.
2	Дополнительная литература	Электронно-библиотечная система издательства Лань	Бондаренко, И. С. Методы и средства защиты информации : учебное пособие / И. С. Бондаренко, Ю. В. Демчишин. — Москва : МИСИС, 2018. — 32 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/115269 (дата обращения: 09.01.2022). — Режим доступа: для авториз. пользователей.
3	Основная литература	Электронно-библиотечная система издательства Лань	Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии : учебник / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2019. — 344 с. — ISBN 978-5-8114-3940-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/125739 (дата обращения: 09.01.2022). — Режим доступа: для авториз. пользователей.
4	Дополнительная литература	Электронно-библиотечная система издательства Лань	Пржегорлинский, В. Н. Объекты защиты информации : учебное пособие / В. Н. Пржегорлинский. — Рязань : РГРТУ, 2012 — Часть 1 : Элементарные объекты защиты информации — 2012. — 132 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/168181 (дата обращения: 09.01.2022). — Режим доступа: для авториз. пользователей.
5	Дополнительная литература	Электронно-библиотечная система издательства Лань	Пржегорлинский, В. Н. Объекты защиты информации : учебное пособие / В. Н. Пржегорлинский. — Рязань : РГРТУ, 2014 — Часть 2 : Комплексные объекты защиты информации — 2014. — 64 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/168180 (дата обращения: 09.01.2022). — Режим доступа: для авториз. пользователей.
6	Дополнительная 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: 09.01.2022). — Режим доступа: для авториз. пользователей.

9. Информационные технологии, используемые при осуществлении образовательного процесса

Перечень используемого программного обеспечения:

1. Microsoft-Windows(бессрочно)
2. Microsoft-Office(бессрочно)
3. -Dia Diagram Editor(бессрочно)

Перечень используемых информационных справочных систем:

1. ООО "ГарантУралСервис"-Гарант(бессрочно)

10. 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+.
Практические занятия и семинары	911 (3б)	Комплект компьютерного оборудования, минитор, маршрутизатор, программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozila Firefox, Консультант+; Операционные системы семейства Linux, Windows, СУБД промышленного масштаба (например, Microsoft SQL Server 2010, Oracle 9i и т.п), свободно распространяемые пакеты прикладных программ: утилиты резервного копирования и восстановления файловых систем и разделов НЖМД; средства диагностики и тестирования ПК; межсетевые экраны; системы обнаружения вторжений; антивирусы.