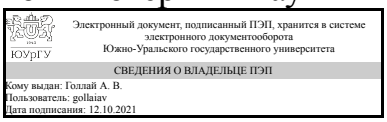
ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Директор института
Высшая школа электроники и компьютерных наук



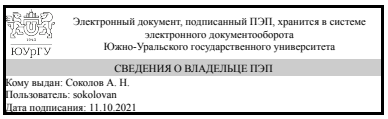
А. В. Голлай

РАБОЧАЯ ПРОГРАММА

дисциплины П.1.В.06.02 Методы исследования защищенности объектов информатизации
для направления 10.06.01 Информационная безопасность
уровень аспирант **тип программы**
направленность программы
форма обучения заочная
кафедра-разработчик Защита информации

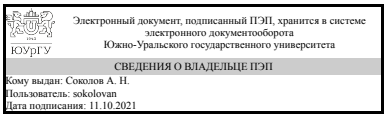
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.06.01 Информационная безопасность, утверждённым приказом Минобрнауки от 29.07.2014 № 874

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

Целями изучения дисциплины являются: - формирование знаний о теоретических и практических подходах к анализу защищенности объектов автоматизации, методологических подходах к исследованию защищенности автоматизированных систем, а также о технологическом и методическом инструментарии исследования защищенности объектов от информационных атак; - освоение научно-исследовательских практик оценки защищенности информационных ресурсов и систем; - знакомство с перспективными направлениями разработки новых методов исследования защищенности информационных ресурсов и систем. Задачи изучения дисциплины: - освоение теоретических основ исследования защищенности объектов информатизации; - формирование знаний о методологическом аппарате анализа процессов обеспечения информационной безопасности и защиты информации; - развитие навыков аналитической и научно-исследовательской деятельности в области изучения защищенности автоматизированных систем, информационных ресурсов и защищаемых объектов информатизации.

Краткое содержание дисциплины

Информационная безопасность и защита информации на объектах информатизации. Формализация объекта информатизации с точки зрения защищенности. Формы и способы комплексной оценки защищенности объекта информатизации. Методы исследования защищенности объектов информатизации. Способы и формы классификации объектов информатизации. Моделирование атак на информационные ресурсы объектов информатизации. Методологические подходы анализа защищенности объектов информатизации на основе формальных и эталонных моделей. Научно-исследовательские подходы к формированию методов исследования защищенности объектов информатизации.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине (ЗУНы)
ОПК-1 способностью формулировать научные задачи в области обеспечения информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность	Знать:современные достижения науки и передовые технологии в области защиты информации и анализа защищенности объектов информатизации
	Уметь:проводить комплексное исследование защищенности объектов информатизации
	Владеть:навыками проведения анализа защищенности с применением различных методологических подходов
ПК-1.1 способностью анализировать теоретические подходы к определению информационной безопасности объектов информатизации	Знать:основные методологические подходы к проведению исследования защищенности объектов информатизации
	Уметь:пользоваться существующим методологическим аппаратом для формирования подходов к анализу защищенности объектов информатизации
	Владеть:методами анализа теоретических

	подходов к определению информационной безопасности объектов информатизации
ОПК-3 способностью обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности	Знать:действующие стандарты в области информационной безопасности
	Уметь:оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности
	Владеть:технологическим и методическим инструментарием процессов оценки защищенности объектов информатизации

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Научно-исследовательская деятельность (1 семестр)	П.1.В.07.02 Программные алгоритмы защиты информации, Научно-исследовательская деятельность (4 семестр), Научно-исследовательская деятельность (3 семестр)

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

Дисциплина	Требования
Научно-исследовательская деятельность (1 семестр)	Знать: методы и средства анализа обработки информации, обеспечения информационной безопасности. Уметь: формулировать новые и совершенствовать существующие методы и средства анализа обработки информации, обеспечения информационной безопасности.

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
		2
Общая трудоёмкость дисциплины	108	108
Аудиторные занятия:	8	8
Лекции (Л)	8	8
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	0	0
Лабораторные работы (ЛР)	0	0

Самостоятельная работа (СРС)	100	100
Подбор и изучение литературных источников, работа с периодической печатью, подготовка тематических обзоров по периодике	26	26
Подготовка к участию в научно-практических конференциях	26	26
Самостоятельное изучение теоретического материала. Методологические подходы анализа защищенности объектов информатизации на основе формальных и эталонных моделей. Формализация данных и способы определения уровней защищенности	48	48
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 и защита информации на объектах информатизации	2	2	0	0
2	Методы исследования защищенности объектов информатизации	4	4	0	0
3	Прикладной и методологический инструментарий исследования защищенности объектов информатизации	2	2	0	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Цели и задачи курса. Содержание дисциплины. Рекомендуемая литература. Объект информатизации как предмет защиты. Свойства и характеристики. Формализация объекта как независимой системы. Основные теоретические подходы и принципы обеспечения информационной безопасности объектов информатизации. Угрозы, уязвимости и способы эксплуатации. Формализация объекта информатизации с точки зрения защищенности. Алгоритмизация характеристик и свойств. Определение защищенности. Формы и способы комплексной оценки защищенности объекта информатизации. Критерии защищенности, способы их измерения и оценки. Методологические подходы к изучению безопасности информации на объектах информатизации.	2
2	2	Методы исследования защищенности объектов информатизации. Основные научные, научно-исследовательские подходы к изучению объектов информатизации с точки зрения безопасности информации. Способы и формы классификации объектов информатизации. Формальные модели защищенности объектов информатизации. Эталонные модели защищенности объектов информатизации. Моделирование атак на информационные ресурсы объектов информатизации. Формализация угроз и уязвимостей как свойств модели. Алгоритмизация атак. Анализ защищенности объекта.	2
3	2	Формальные и эталонные модели в анализе защищенности объектов информатизации. Сравнительный анализ защищенности объектов информатизации. Способы нормализации моделей. Прямая и обратная задачи моделирования объекта информатизации с точки зрения исследования защищенности. Научно-исследовательские подходы к формированию методов исследования защищенности объектов информатизации. Аналитический аппарат формирования методов и прикладного	2

		инструментария для целей исследования защищенности объектов информатизации. Оценка результатов исследования защищенности объектов информатизации. Методы экспертной оценки, проверки на адекватность и аналитической декомпозиции моделей объектов информатизации.	
4	3	Прикладной и методологический инструментарий исследования защищенности объектов информатизации. Отечественный и зарубежный опыт исследования защищенности объектов информатизации. Сравнительный анализ существующих прикладных и методологических инструментов анализа защищенности объектов информатизации. Изучение основных принципов формирования аналитических средств исследования. Перспективы развития научно-исследовательского и методологического аппаратов исследования защищенности объектов информатизации.	2

5.2. Практические занятия, семинары

Не предусмотрены

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
Самостоятельное изучение теоретического материала. Методологические подходы анализа защищенности объектов информатизации на основе формальных и эталонных моделей. Формализация данных и способы определения уровней защищенности	Основная и дополнительная литература по дисциплине. Периодические издания, раскрывающие вопросы исследования защищенности объектов информатизации	48
Подготовка к участию в научно-практических конференциях	Основная и дополнительная литература по дисциплине. Периодические издания, раскрывающие вопросы исследования защищенности объектов информатизации	26
Подбор и изучение литературных источников, работа с периодической печатью, подготовка тематических обзоров по периодике	Основная и дополнительная литература по дисциплине. Периодические издания, раскрывающие вопросы исследования защищенности объектов информатизации	26

6. Инновационные образовательные технологии, используемые в учебном процессе

Инновационные формы учебных занятий	Вид работы (Л, ПЗ, ЛР)	Краткое описание	Кол-во ауд. часов
Разбор конкретных ситуаций	Лекции	Сравнительный анализ существующих прикладных и методологических инструментов анализа защищенности объектов информатизации. Изучение основных принципов	2

		формирования аналитических средств исследования	
Разбор конкретных ситуаций	Лекции	Прикладной и методологический инструментарий исследования защищенности объектов информатизации. Отечественный и зарубежный опыт исследования защищенности объектов информатизации	2

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
Все разделы	ОПК-1 способностью формулировать научные задачи в области обеспечения информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность	Экзамен	1 - 18
Все разделы	ОПК-3 способностью обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности	Экзамен	1 - 18
Все разделы	ПК-1.1 способностью анализировать теоретические подходы к определению информационной безопасности объектов информатизации	Экзамен	1 - 18

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. Информационная безопасность и защита информации на объектах информатизации. Основные понятия 2. Объект информатизации как предмет защиты. Свойства и характеристики. Формализация объекта как независимой системы 3. Основные теоретические подходы и принципы обеспечения информационной безопасности объектов информатизации. Угрозы, уязвимости и способы эксплуатации 4. Формализация объекта информатизации с точки зрения защищенности. Алгоритмизация характеристик и свойств. Определение защищенности 5. Формы и способы комплексной оценки защищенности объекта информатизации. Критерии защищенности, способы их измерения и оценки. Методологические подходы к изучению безопасности информации на объектах информатизации 6. Методы исследования защищенности объектов информатизации. Основные научные, научно-исследовательские подходы к изучению объектов информатизации с точки зрения безопасности информации 7. Способы и формы классификации объектов информатизации. Формальные и эталонные модели защищенности объектов информатизации 8. Моделирование атак на информационные ресурсы объектов информатизации. Алгоритмы изучения эксплуатации уязвимостей объектов информатизации. Анализ защищенности объекта 9. Сравнительный анализ защищенности объектов информатизации. Способы нормализации моделей. Пряма и обратная задача моделирования объекта информатизации с точки зрения исследования защищенности 10. Научно-исследовательские подходы к формированию методов исследования защищенности объектов информатизации. Аналитический аппарат формирования методов и прикладного инструментария для целей исследования защищенности объектов информатизации 11. Оценка результатов исследования защищенности объектов информатизации. Методы экспертной оценки, проверки на адекватность и аналитической декомпозиции моделей объектов информатизации 12. Информационная безопасность и защита информации на объектах информатизации. Основные понятия 13. Объект информатизации как предмет защиты. Свойства и характеристики. Формализация объекта как независимой системы 14. Основные теоретические подходы и принципы обеспечения информационной безопасности объектов информатизации. Угрозы, уязвимости и способы эксплуатации 15. Формализация объекта информатизации с точки зрения защищенности. Алгоритмизация характеристик и свойств. Определение защищенности 16. Формы и способы комплексной оценки защищенности объекта информатизации. Критерии защищенности, способы их измерения и оценки. Методологические подходы к изучению безопасности информации на объектах информатизации

	17. Методы исследования защищенности объектов информатизации. Основные научные, научно-исследовательские подходы к изучению объектов информатизации с точки зрения безопасности информации 18. Способы и формы классификации объектов информатизации. Формальные и эталонные модели защищенности объектов информатизации

8. Учебно-методическое и информационное обеспечение дисциплины

Печатная учебно-методическая документация

а) основная литература:

1. Волкова, В. Н. Теория систем и системный анализ [Текст] учебник для вузов по направлению 010502 (351400) "Прикл. информатика" В. Н. Волкова, А. А. Денисов. - 2-е изд., перераб. и доп. - М.: Юрайт, 2013. - 616 с. ил.
2. Качала, В. В. Основы теории систем и системного анализа [Текст] учеб. пособие для вузов по специальности "Приклад. информатика (по областям)" В. В. Качала. - 2-е изд., испр. - М.: Горячая линия - Телеком, 2015. - 210 с. ил.
3. Прохорова, И. А. Теория систем и системный анализ [Текст] учеб. пособие по направлению "Приклад. информатика" И. А. Прохорова ; Юж.-Урал. гос. ун-т, Каф. Информатика ; ЮУрГУ. - Челябинск: Издательский Центр ЮУрГУ, 2013. - 48, [1] с. ил. электрон. версия

б) дополнительная литература:

1. Северцев, Н. А. Системный анализ и моделирование безопасности [Текст] учеб. пособие для вузов по направлению 656500 (280100) "Безопасность жизнедеятельности" Н. А. Северцев, В. К. Дедков. - М.: Высшая школа, 2006. - 461, [1] с.

в) отечественные и зарубежные журналы по дисциплине, имеющиеся в библиотеке:

1. Вестник УрФО. Безопасность в информационной сфере
2. BIS Journal-Информационная безопасность банков
3. Безопасность информационных технологий
4. Бизнес и безопасность в России
5. Вестник ИТАРК
6. Вестник РГГУ. Серия: Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность
7. Вопросы защиты информации
8. Вопросы кибербезопасности
9. Защита информации. Инсайд
10. Информатика и математические методы в моделировании
11. Информационная безопасность и компьютерные технологии в деятельности правоохранительных органов
12. Информационная безопасность социотехнических систем
13. Информационное противодействие угрозам терроризма
14. Информационные и математические технологии в науке и управлении
15. Информационные технологии
16. Информационные технологии и управление

17. ИТ Арктика
18. ИТНОУ: Информационные технологии в науке, образовании и управлении
19. Компьютерная оптика
20. Математические структуры и моделирование
21. Методы и технические средства обеспечения безопасности информации
22. Национальная безопасность и стратегическое планирование
23. Охрана, безопасность, связь
24. Правовая информатика
25. Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений
26. Проблемы правовой и технической защиты информации
27. Программная инженерия и информационная безопасность
28. Системы управления, связи и безопасности
29. Специальная техника
30. Спецтехника и связь
31. Управление защитой информации
32. Управление информационными рисками и обеспечение безопасности инфокоммуникационных систем
33. Ученые записки УлГУ. Серия: Математика и информационные технологии

г) методические указания для студентов по освоению дисциплины:

1. Царегородцев А.В. Математическое моделирование управляющих систем: Методическое пособие. – М.: Изд-во РУДН, 2003., 80 с.

из них: учебно-методическое обеспечение самостоятельной работы студента:

1. Царегородцев А.В. Математическое моделирование управляющих систем: Методическое пособие. – М.: Изд-во РУДН, 2003., 80 с.

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
1	Дополнительная литература	Электронно-библиотечная система издательства Лань	Зайцев, А. П. Технические средства и методы защиты информации : учебник / А. П. Зайцев, Р. В. Мещеряков, А. А. Шелупанов. — 7-е изд., испр. — Москва : Горячая линия-Телеком, 2018. — 442 с. — ISBN 978-5-9912-0233-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111057 (дата обращения: 11.10.2021). — Режим доступа: для авториз. пользователей.
2	Основная литература	Электронная библиотека Юрайт	Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2021. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст :

			электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/469866 (дата обращения: 11.10.2021).
3	Дополнительная литература	Электронно-библиотечная система издательства Лань	Рагозин, Ю. Н. Инженерно-техническая защита информации на объектах информатизации : учебное пособие / Ю. Н. Рагозин. — Санкт-Петербург : Интермедия, 2019. — 216 с. — ISBN 978-5-4383-0182-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/161337 (дата обращения: 11.10.2021). — Режим доступа: для авториз. пользователей.
4	Основная литература	Электронная библиотека Юрайт	Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2021. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/471159 (дата обращения: 11.10.2021).

9. Информационные технологии, используемые при осуществлении образовательного процесса

Перечень используемого программного обеспечения:

1. Microsoft-Office(бессрочно)

Перечень используемых информационных справочных систем:

1. -Стандартинформ(бессрочно)
2. -База данных ВИНИТИ РАН(бессрочно)
3. -Информационные ресурсы ФИПС(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+