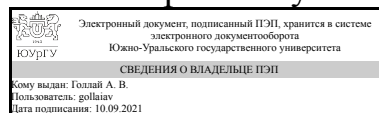


# ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ  
Директор института  
Высшая школа электроники и  
компьютерных наук



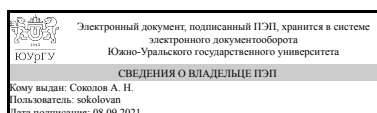
А. В. Голлай

## РАБОЧАЯ ПРОГРАММА научных исследований к ОП ВО от 30.06.2021 №084-2133

Научно-исследовательская деятельность  
для направления 10.06.01 Информационная безопасность  
Уровень подготовка кадров высшей квалификации  
направленность программы Методы и системы защиты информации,  
информационная безопасность (05.13.19)  
форма обучения очная  
кафедра-разработчик Защита информации

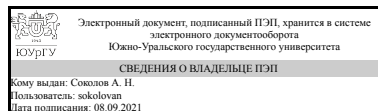
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.06.01 Информационная безопасность, утверждённым приказом Минобрнауки от 29.07.2014 № 874

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



А. Н. Соколов

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



А. Н. Соколов

# 1. Общая характеристика

## Форма проведения

Непрерывно

## Цель научных исследований

Проведение теоретических и вычислительных работ по разработке методов решения поставленных задач диссертационного исследования и сопряженных задач.

## Задачи научных исследований

1. Разработка алгоритмов решения задач диссертационного исследования.
2. Отработка алгоритмов решения задач диссертационного исследования на основе их программирования.

## Краткое содержание научных исследований

1. Апробация концепции решения общей задачи диссертационного исследования и сопряженных задач на основе аналитических исследований и вычислительных экспериментов.
2. Разработка алгоритмов решения задач диссертационного исследования.
3. Отработка алгоритмов решения задач диссертационного исследования на основе их программирования.
4. Проведение оценок эффективности предлагаемых методов и алгоритмов решения задач диссертационного исследования на основе сравнения с опытными данными.

## 2. Компетенции обучающегося, формируемые в результате выполнения научных исследований

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения при прохождении практики (ЗУНы)
ПК-1.2 способностью исследовать методологические подходы обеспечения информационной безопасности и применять их при разработке систем защиты информации	Знать: существующие методы и средства, применяемые для анализа систем защиты информации.
	Уметь: анализировать методы и средства, применяемые для создания систем защиты информации; разрабатывать предложения по их совершенствованию и повышению эффективности.
	Владеть: навыками анализа и разработки методов и средств, применяемых для создания систем защиты информации.
УК-1 способностью к критическому анализу и оценке современных научных достижений, генерированию новых идей при решении исследовательских и практических задач, в том числе в	Знать: Методы критического анализа и оценки современных научных достижений, а также методы генерирования новых идей при исследовательских и практических задач.

междисциплинарных областях	Уметь: Уметь анализировать альтернативные варианты решения исследовательских и практических задач и оценивать потенциальные выигрыши/проигрыши реализации этих вариантов.
	Владеть: Методами экспертного анализа и оценки современных научных достижений при решении исследовательских и практических задач, в том числе в междисциплинарных областях.
ОПК-2 способностью разрабатывать частные методы исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности	Знать: частные методы исследования в области обеспечения информационной безопасности
	Уметь: применять частные методы исследования в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности
	Владеть: использования частных методов исследования в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности

### 3. Место научных исследований в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ	Перечень последующих дисциплин, видов работ
Методы и системы защиты информации, информационная безопасность Научно-исследовательская деятельность (1 семестр)	Моделирование информационного противодействия угрозам безопасности информации Научно-исследовательская деятельность (4 семестр) Научно-исследовательская деятельность (3 семестр)

Требования к «входным» знаниям, умениям, навыкам аспиранта, необходимым для выполнения научных исследований и приобретенным в результате освоения предшествующих дисциплин:

Дисциплина	Требования
Методы и системы защиты информации, информационная безопасность	Знать: теоретические подходы к определению информационной безопасности объектов информатизации.

	Уметь: определять характеристики информационной безопасности объектов информатизации. Владеть: навыками анализа и разработки методов определения информационной безопасности объектов информатизации.
Научно-исследовательская деятельность (1 семестр)	Утвержденная тема научно-квалификационной работы (диссертации).

#### 4. Время проведения

Время проведения научных исследований (номер уч. недели в соответствии с графиком) с 23 по 42

#### 5. Этапы и объем научных исследований

Общая трудоемкость составляет зачетных единиц 21, часов 756, недель 14.

№ раздела (этапа)	Наименование разделов (этапов)	Кол-во часов	Форма текущего контроля
3	Подготовка к докладу на кафедре	56	Доклад на кафедре
1	Разработка алгоритмов решения задач диссертационного исследования	300	Доклад на кафедре
2	Отработка алгоритмов решения задач диссертационного исследования на основе их программирования	400	Доклад на кафедре

#### 6. Содержание научных исследований

№ раздела (этапа)	Наименование или краткое содержание вида работ	Кол-во часов
1.1	Проведение обзора и самостоятельных образовательных работ по освоению современного состояния научно-практических исследований в предметной области диссертационной работы.	100
1.2	Апробация концепции решения общей задачи диссертационного исследования и сопряженных задач на основе аналитических исследований и вычислительных экспериментов. Разработка алгоритмов решения задач диссертационного исследования	200
3	Подготовка к докладу на кафедре	56
2.2	Отработка алгоритмов решения задач диссертационного исследования на основе их программирования. Проведение оценок эффективности предлагаемых методов и алгоритмов решения задач диссертационного исследования на основе сравнения с	200

	Опытными данными	
2.1	Проведение научно-исследовательских работ по выявлению и анализу проблемных вопросов в предметной области диссертационной работы на основе обзора литературы и установление контактов с предприятиями (организациями) с целью выявления нерешенных научно-практических задач для соответствующих технологий обеспечения информационной безопасности	200

## 7. Формы отчетности

В течении семестра аспирант делает доклад на кафедре об основных результатах научно-исследовательской деятельности.

## 8. Фонд оценочных средств для проведения промежуточной аттестации

Форма итогового контроля – зачет.

### 8.1. Паспорт фонда оценочных средств

Наименование разделов	Код контролируемой компетенции (или ее части)	Вид контроля
Все разделы	УК-1 способностью к критическому анализу и оценке современных научных достижений, генерированию новых идей при решении исследовательских и практических задач, в том числе в междисциплинарных областях	Доклад на кафедре
Все разделы	ОПК-2 способностью разрабатывать частные методы исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности	Зачет
Все разделы	ПК-1.2 способностью исследовать методологические подходы обеспечения информационной безопасности и применять их при разработке систем защиты информации	Доклад на кафедре
Все разделы	ПК-1.2 способностью исследовать методологические подходы обеспечения информационной безопасности и применять их при разработке систем защиты информации	Зачет
Все разделы	УК-1 способностью к критическому анализу и оценке современных научных достижений, генерированию новых идей при решении исследовательских и практических задач, в том числе в междисциплинарных областях	Зачет
Все разделы	ОПК-2 способностью разрабатывать частные методы исследования и применять их в самостоятельной научно-исследовательской деятельности для решения	Доклад на кафедре

	конкретных исследовательских задач в области обеспечения информационной безопасности	
--	--	--

## 8.2. Виды контроля, процедуры проведения, критерии оценивания

Вид контроля	Процедуры проведения и оценивания	Критерии оценивания
Зачет	<p>Зачет проводится научным руководителем аспиранта по результатам выполнения исследовательской составляющей индивидуального плана работы аспиранта за семестр с учетом результатов доклада на кафедре. По результатам зачета научный руководитель выставляет 2-балльную (недифференцированную) оценку.</p>	<p>Зачтено: исследовательская составляющая индивидуального плана работы аспиранта за семестр выполнена. Не зачтено: исследовательская составляющая индивидуального плана работы аспиранта за семестр не выполнена.</p>
Доклад на кафедре	<p>В течение семестра аспирант должен выполнить аналитический обзор имеющихся научных публикаций в предметной области исследований по результатам выполнения алгоритмов и освоить необходимые инструменты решения задач по утвержденной теме диссертации. На кафедре проводится научный семинар, в ходе которого аспирант делает доклад о результатах выполненной работы. Структура доклада должна соответствовать общепринятой структуре научных публикаций. Тема доклада должна быть сформулирована аспирантом компактно, все аспекты темы должны быть представлены в докладе. Доклад должен содержать вводную часть (актуальность, научную новизну и значимость; объект и предмет исследования; цели и задачи исследования), основную часть (описание используемых методов, ход работы и ее результаты) и заключение (выводы по проделанной работе). Общая продолжительность доклада должна составлять 7 – 10 минут. Доклад должен сопровождаться презентацией. Презентация не должна дублировать текст доклада и, в зависимости от продолжительности доклада и объема материала, может содержать 7 – 20 слайдов (0,5 – 1 минута доклада на слайд).</p>	<p>Зачтено: аспирант сделал доклад на кафедре в соответствии с установленной процедурой. Не зачтено: аспирант не сделал доклад на кафедре, либо сделанный доклад не соответствует установленным требованиям.</p>

	<p>Слайды презентации, сопровождающие доклад, должны содержать рисунки, схемы, диаграммы, графики, таблицы, списки и другие элементы, помогающие сформулировать представление у аудитории о проделанной работе и ее результатах. Доклад оценивается комиссией, назначенной заведующим кафедрой из числа сотрудников кафедры. По итогам выступления комиссия выставляет 2-балльную (недифференцированную) оценку.</p>	
--	--	--

### 8.3. Примерная тематика научных исследований

- 3. Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса.
- 15. Модели и методы управления информационной безопасностью.
- 8. Модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем.
- 9. Модели и методы оценки защищенности информации и информационной безопасности объекта.
- 1. Теория и методология обеспечения информационной безопасности и защиты информации.
- 11. Технологии идентификации и аутентификации пользователей и субъектов информационных процессов. Системы разграничения доступа.
- 13. Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.
- 6. Модели и методы формирования комплексов средств противодействия угрозам хищения (разрушения, модификации) информации и нарушения информационной безопасности для различного вида объектов защиты вне зависимости от области их функционирования.
- 12. Мероприятия и механизмы формирования политики обеспечения информационной безопасности для объектов всех уровней иерархии системы управления.
- 7. Анализ рисков нарушения информационной безопасности и уязвимости процессов переработки информации в информационных системах любого вида и области применения.
- 5. Методы и средства (комплексы средств) информационного противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет.
- 10. Модели и методы оценки эффективности систем (комплексов) обеспечения информационной безопасности объектов защиты.
- 14. Модели, методы и средства обеспечения внутреннего аудита и мониторинга состояния объекта, находящегося под воздействием угроз нарушения его информационной безопасности.
- 4. Системы документооборота (вне зависимости от степени их компьютеризации) и

средства защиты циркулирующей в них информации.

2. Методы, аппаратно-программные и организационные средства защиты систем (объектов) формирования и предоставления пользователям информационных ресурсов различного вида.

## 9. Учебно-методическое и информационное обеспечение

### Печатная учебно-методическая документация

#### *а) основная литература:*

1. Баранова, Е. К. Информационная безопасность и защита информации [Текст] учеб. пособие по направлению "Приклад. информатика" Е. К. Баранова, А. В. Бабаш. - 3-е изд., перераб. и доп. - М.: РИОР : ИНФРА-М, 2016. - 320, [1] с. ил.
2. Грибунин, В. Г. Комплексная система защиты информации на предприятии [Текст] учеб. пособие для вузов по специальностям "Орг. и технология защиты информации" и др. В. Г. Грибунин, В. В. Чудовский. - М.: Академия, 2009. - 411, [1] с. ил., табл.
3. Малюк, А. А. Информационная безопасность: концептуальные и методологические основы защиты информации Учеб. пособие для вузов по специальности 075400 "Комплекс. защита объектов информации" А. А. Малюк. - М.: Горячая линия - Телеком, 2004. - 280 с. ил.

#### *б) дополнительная литература:*

1. Ажмухамедов, И. М. Управление слабоформализуемыми социотехническими системами на основе нечеткого когнитивного моделирования (на примере систем комплексного обеспечения информационной безопасности) [Текст] автореф. дис. ...д-ра. техн. наук : Специальность 05.13.01 – Системный анализ, управление и обработка информации (промышленность, информатика) ; 05.13.19 – Методы и системы защиты информации, информационная безопасность И. М. Ажмухамедов ; науч. консультант О. М. Проталинский ; Астрахан. гос. техн. ун-т. - Астрахань, 2014. - 31 с.
2. Бабаш, А. В. Информационная безопасность. История защиты информации в России [Текст] учеб. пособие для вузов по направлениям "Информ. безопасность" и "Приклад. информатика" А. В. Бабаш, Е. К. Баранова, Д. А. Ларин. - М.: КноРус, 2015
3. Боровский, А. С. Модели, методы и алгоритмы интеллектуальной поддержки принятия решений в задачах разработки и оценки систем физической защиты объектов информатизации [Текст] автореф. дис. ... д-ра техн. наук : специальность 05.13.19 - Методы и системы защиты информации, информационная безопасность А. С. Боровский ; науч. консультант А. В. Суханов ; Оренбург. гос. аграр. ун-т. - СПб., 2015. - 34 с. ил.
4. Девянин, П. Н. Модели безопасности компьютерных систем Учеб. пособие для вузов по специальностям 075200 "Компьютер. безопасность" и 075500 "Комплексное обеспечение информац. безопасности автоматизир. систем" П. Н. Девянин. - М.: Academia, 2005. - 142, [1] с.



5. Конеев, И. Р. Информационная безопасность предприятия [Текст] И. Р. Конеев, А. В. Беляев. - СПб.: БХВ-Петербург, 2003. - 733 с. ил.
6. Мельников, В. П. Защита информации [Текст] учебник для вузов по направлению 230100 "Информатика и вычисл. техника" (бакалавриат) В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе ; под ред. В. П. Мельникова. - М.: Академия, 2014. - 296 с. ил.
7. Политов, М. С. Экспериментально-аналитический метод оценки и прогнозирования уровня защищенности информационных систем на основе модели временных рядов [Текст] Автореф. дис. ... канд. техн. наук : Специальность 05.13.19 - Методы и системы защиты информации, информационная безопасность М. С. Политов ; науч. рук. А. В. Мельников ; Челяб. гос. ун-т. - Уфа, 2010. - 16 с. ил.
8. Титова, Е. М. Метод противодействия перехвату информации на основе зашумления канала передачи с использованием сверточных кодов [Текст] Автореф. дис. ... канд. техн. наук : Специальность 05.13.19 - Методы и системы защиты информации, информационная безопасность Е. М. Титова ; науч. рук. Е. Т. Мирончиков ; Петербург. гос. ун-т путей сообщения. - Санкт-Петербург, 2010. - 16 с.
9. Вестник УрФО : Безопасность в информационной сфере Юж.-Урал. гос. ун-т; ЮУрГУ журнал. - Челябинск: Издательство ЮУрГУ, 2011-

*из них методические указания для самостоятельной работы студента:*

Не предусмотрена

### **Электронная учебно-методическая документация**

№	Вид литературы	Наименование разработки	Наименование ресурса в электронной форме	Доступность (сеть Интернет / локальная сеть; авторизованный / свободный доступ)
1	Основная литература	База текстов статей ScienceDirect ( <a href="https://www.sciencedirect.com/">https://www.sciencedirect.com/</a> )	ScienceDirect	Интернет / Авторизованный
2	Основная литература	База текстов статей IEEE Xplore Digital Library ( <a href="https://ieeexplore.ieee.org/">https://ieeexplore.ieee.org/</a> )	IEEE Xplore Digital Library	Интернет / Авторизованный
3	Дополнительная литература	Научная электронная библиотека (РИНЦ) eLIBRARY.RU ( <a href="https://elibrary.ru/">https://elibrary.ru/</a> )	eLIBRARY.RU	Интернет / Авторизованный

### **10. Информационные технологии, используемые при выполнении научных исследований**

Перечень используемого программного обеспечения:

1. Microsoft-Office(бессрочно)

Перечень используемых информационных справочных систем:

1. ООО "ГарантУралСервис"-Гарант(бессрочно)

2. -Стандартинформ(бессрочно)
3. -База данных ВИНТИ РАН(бессрочно)
4. -Информационные ресурсы ФИПС(бессрочно)

## 11. Материально-техническое обеспечение

<b>Место выполнения научных исследований</b>	<b>Адрес</b>	<b>Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение</b>
Кафедра "Защита информации" ЮУрГУ	454080, Челябинск, Ленина, 87	Оборудование и компьютеры лабораторий кафедры, собственный ноутбук аспиранта