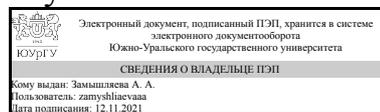


# ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:  
Директор института  
Институт естественных и точных  
наук



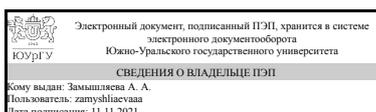
А. А. Замышляева

## РАБОЧАЯ ПРОГРАММА

**дисциплины** 1.Ф.П2.02 Математическое моделирование и прогнозирование информационных угроз  
**для направления** 01.03.02 Прикладная математика и информатика  
**уровень** Бакалавриат  
**профиль подготовки** Математические методы обеспечения безопасности программных систем  
**форма обучения** очная  
**кафедра-разработчик** Прикладная математика и программирование

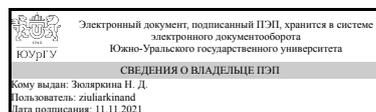
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 01.03.02 Прикладная математика и информатика, утверждённым приказом Минобрнауки от 10.01.2018 № 9

Зав.кафедрой разработчика,  
д.физ.-мат.н., проф.



А. А. Замышляева

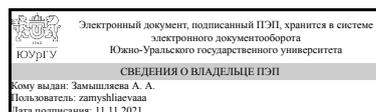
Разработчик программы,  
д.физ.-мат.н., доц., профессор



Н. Д. Зюляркина

СОГЛАСОВАНО

Руководитель образовательной  
программы  
д.физ.-мат.н., проф.



А. А. Замышляева

## 1. Цели и задачи дисциплины

Цель дисциплины - освоение дисциплинарных компетенций по применению комплекса мероприятий в системе защиты информации на основе технологии прогнозирования рисков информационной безопасности. Задачи дисциплины: - разработка и исследование алгоритмов, вычислительных моделей и моделей данных для реализации элементов новых (или известных) сервисов систем информационных технологий; - формирование способности произвести и детально обосновать выбор структуры, принципов организации, комплекса средств и технологий обеспечения информационной безопасности объектов защиты; - формирование способности разрабатывать и исследовать аналитические и структурные модели техники защиты информации и её компонентов.

## Краткое содержание дисциплины

Основы прогнозирования рисков информационной безопасности, требования к системе управления рисками информационной безопасности, управление рисками в системе информационной безопасности.

## 2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине
ПК-6 Способен использовать математические методы при проектировании и разработке алгоритмических и программных решений в области обеспечения безопасности и защиты программных систем.	Знает: стандарты в области управления рисками информационной безопасности Умеет: применять программное обеспечение для оценки рисков информации-онной безопасности Имеет практический опыт: подбора инструментальных средств для управления информацией-онными рисками

## 3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Теория информации и кодирования, Ассемблер в задачах защиты информации, Математические основы криптографии, Криптографические методы защиты информации	Не предусмотрены

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

Дисциплина	Требования
Теория информации и кодирования	Знает: способы формирования оптимальных кодов в системе передачи информации Умеет: Имеет практический опыт: оценки предельных возможностей информационных систем, оптимального кодирования и передачи сигналов

Математические основы криптографии	Знает: алгебраические структуры, лежащие в основе современных криптографических систем Умеет: использовать математические методы при создании криптографических спецификаций Имеет практический опыт:
Ассемблер в задачах защиты информации	Знает: технологии исследования программных алгоритмов Умеет: выстраивать систему защиты программы Имеет практический опыт: программирования на языке ассемблер, дизассемблирования и отладки программ
Криптографические методы защиты информации	Знает: принципы построения криптографических алгоритмов, криптографические стандарты, основные подходы к реализации криптографических средств защиты информации Умеет: Имеет практический опыт: решения задач, связанных с распределением ключевой информации, шифрованием чувствительной информации и цифровой подписью сообщений

#### 4. Объём и виды учебной работы

Общая трудоёмкость дисциплины составляет 3 з.е., 108 ч., 66,25 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах	
		Номер семестра	
		8	
Общая трудоёмкость дисциплины	108	108	
<i>Аудиторные занятия:</i>	60	60	
Лекции (Л)	24	24	
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	0	0	
Лабораторные работы (ЛР)	36	36	
<i>Самостоятельная работа (СРС)</i>	41,75	41,75	
с применением дистанционных образовательных технологий	0		
Подготовка к лабораторным работам. Оформление отчётов.	31,75	31.75	
Подготовка к зачету	10	10	
Консультации и промежуточная аттестация	6,25	6,25	
Вид 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	Основы прогнозирования рисков информационной безопасности	12	4	0	8
2	Требования к системе управления рисками	24	8	0	16

	информационной безопасности				
3	Управление рисками в системе информационной безопасности	24	12	0	12

## 5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1-2	1	Основные понятия, термины и определения. Предмет и задачи дисциплины. Цели и задачи курса и его место в подготовке студентов. Особенности формирования терминологии научной дисциплины. Взаимосвязь курса с другими дисциплинами учебного плана. Методические материалы. Периодические издания. Обязательная и дополнительная литература. Современные информационные риски и их особенности. Кибертерроризм. Риски промышленных систем. Риски утечки информации. Риски электронных расчётов. Стандарты управления рисками. Государственное регулирование. Оценка рисков как основа корпоративного управления.	4
3-4	2	Стандарты в области управления рисками информационной безопасности. Понятие риска. Оценка риска. Количественное определение величины риска. Качественное определение величины риска. Информационная составляющая бизнес-рисков. Активы организации как ключевые факторы риска. Подходы к управлению рисками. Уровни зрелости бизнеса в отношении рисков. Анализ факторов риска. Методика оценки рисков приватности, включая персональные данные.	4
5-6	2	О преимуществах системного подхода к управлению рисками. Структура документации по управлению рисками. Политика и контекст управления рисками. Структура системы управления рисками. Процессная модель управления рисками. Непрерывная деятельность по управлению рисками. Сопровождение и мониторинг механизмов безопасности. Анализ со стороны руководства. Пересмотр и переоценка риска. Взаимосвязь процессов аудита и управления рисками. Управление документами и записями. Корректирующие и превентивные меры. Коммуникация рисков. Аутсорсинг процессов управления рисками. Распределение ответственности за управление рисками. Требования к риск-менеджеру. Требования к эксперту по оценке рисков.	4
7-8	3	Идентификация активов. Описание бизнес-процессов. Идентификация требований безопасности. Реестр требований безопасности. Требования законодательства и нормативной базы. Контрактные обязательства. Требования бизнеса. Определение ценности активов. Критерии оценки ущерба. Таблица ценности активов. Особенности интервьюирования бизнес-пользователей. Определение приоритетов аварийного восстановления.	4
9-10	3	Анализ угроз и уязвимостей. Профиль и жизненный цикл угрозы. Описание угроз безопасности. Способы классификации угроз. Уязвимости информационной безопасности. Идентификация организационных уязвимостей. Идентификация технических уязвимостей. Оценка угроз и уязвимостей. Определение величины риска. Калибровка шкалы оценки риска. Пример оценки риска. Отчёт об оценке рисков. Способы обработки риска. Принятие риска. Уменьшение риска. Передача риска. Избегание риска. Оценка возврата инвестиций в информационную безопасность. Принятие решения по обработке риска. План обработки рисков. Декларация о применимости механизмов контроля. Профили рисков информационной безопасности.	4
11-12	3	Актуальность программного сопровождения процедуры оценки рисков. Выбор программного обеспечения для оценки рисков. Общие недостатки и ограничения коммерческих программных продуктов. Обзор методов и	4

		инструментальных средств управления рисками: OCTAVE, CRAMM, RiskWatch, CORBA, RA2 the art of risk, vsRisk, Proteus Enterprise. Особенности внедрения системы управления информационными рисками (СУИР). Документация. Начальные условия для внедрения СУИР. Организационная структура управления рисками. Обучение членов экспертной группы.	
--	--	--	--

## 5.2. Практические занятия, семинары

Не предусмотрены

## 5.3. Лабораторные работы

№ занятия	№ раздела	Наименование или краткое содержание лабораторной работы	Кол-во часов
1-2	1	Лабораторная работа 1. Исследование системы анализа рисков и проверки политики информационной безопасности предприятия	4
3-4	1	Лабораторная работа 1. Исследование системы анализа рисков и проверки политики информационной безопасности предприятия (продолжение)	4
5-6	2	Лабораторная работа 2. Исследование защищенности беспроводных сетей передачи данных	4
7-8	2	Лабораторная работа 2. Исследование защищенности беспроводных сетей передачи данных (продолжение)	4
9-10	2	Лабораторная работа 3. Исследование и администрирование средств обеспечения информационной безопасности Web-сервера Microsoft IIS Server	4
11-12	2	Лабораторная работа 3. Исследование и администрирование средств обеспечения информационной безопасности Web-сервера Microsoft IIS Server (продолжение)	4
13-14	3	Лабораторная работа 4. Исследование и администрирование средств обеспечения информационной безопасности Microsoft ISA Security Server. Установка и конфигурирование брандмауэра ISA. Построение VPN-сети на базе ISA	4
15-16	3	Лабораторная работа 4. Исследование и администрирование средств обеспечения информационной безопасности Microsoft ISA Security Server. Установка и конфигурирование брандмауэра ISA. Построение VPN-сети на базе ISA (продолжение)	4
17-18	3	Лабораторная работа 5. Исследование и развертывание сетевой инфраструктуры Microsoft Windows Exchange Server	4

## 5.4. Самостоятельная работа студента

Выполнение СРС			
Подвид СРС	Список литературы (с указанием разделов, глав, страниц) / ссылка на ресурс	Семестр	Кол-во часов
Подготовка к лабораторным работам. Оформление отчётов.	ЭУМД. осн. лит. п. 1, п. 2, доп. лит. п. 3.	8	31,75
Подготовка к зачету	ЭУМД. осн. лит. п. 1, п. 2, доп. лит. п. 3.	8	10

## 6. Текущий контроль успеваемости, промежуточная аттестация

Контроль качества освоения образовательной программы осуществляется в соответствии с Положением о балльно-рейтинговой системе оценивания результатов учебной деятельности обучающихся.

### 6.1. Контрольные мероприятия (КМ)

№ КМ	Семестр	Вид контроля	Название контрольного мероприятия	Вес	Макс. балл	Порядок начисления баллов	Учитывается в ПА
1	8	Текущий контроль	КМ-1. Контрольная работа 1	12	2	2 балла - верно выполнены все 3 этапа работы. Представлен отчёт. 1 балл - верно выполнены 2 этапа работы. Представлен отчёт. 0 баллов - в остальных случаях.	зачет
2	8	Текущий контроль	КМ-2. Лабораторная работа 2	12	2	2 балла - верно выполнены все этапы работы. Представлен отчёт. 1 балл - верно выполнено не менее 60% этапов работы. Представлен отчёт. 0 баллов - в остальных случаях.	зачет
3	8	Текущий контроль	КМ-3. Лабораторная работа 3	12	2	2 балла - верно выполнены все этапы работы. Представлен отчёт. 1 балл - верно выполнено не менее 60% этапов работы. Представлен отчёт. 0 баллов - в остальных случаях.	зачет
4	8	Текущий контроль	КМ-4. Лабораторная работа 4	12	2	2 балла - верно выполнены все этапы работы. Представлен отчёт. 1 балл - верно выполнено не менее 60% этапов работы. Представлен отчёт. 0 баллов - в остальных случаях.	зачет
5	8	Текущий контроль	КМ-5. Лабораторная работа 5	12	2	2 балла - верно выполнены все этапы работы. Представлен отчёт. 1 балл - верно выполнено не менее 60% этапов работы. Представлен отчёт. 0 баллов - в остальных случаях.	зачет
6	8	Текущий контроль	КМ-6. Активная познавательная деятельность	40	60	На каждом из 30 занятий студент может получить 2 балла: Студент задает вопросы по изучаемому материалу - 1 балл; Студент правильно отвечает на вопросы по изучаемому материалу - 1 балл. В противном случае баллы не начисляются.	зачет
7	8	Промежуточная аттестация	КМ-7. Опрос	1	4	Контрольное мероприятие промежуточной аттестации проводится во время экзамена в виде устного опроса. Студенту задаются 4 вопроса из разных тем курса. Правильный ответ на вопрос - 1 балл; Неправильный ответ на вопрос - 0 баллов.	зачет

### 6.2. Процедура проведения, критерии оценивания

Вид промежуточной аттестации	Процедура проведения	Критерии оценивания
зачет	На зачёте происходит оценивание учебной деятельности обучающихся по дисциплине на основе полученных оценок за контрольно-рейтинговые мероприятия текущего контроля. Студент может улучшить свой рейтинг, пройдя контрольное мероприятие промежуточной аттестации, которое не является обязательным. Контрольное мероприятие промежуточной аттестации проводится во время зачёта в виде устного опроса. Студенту задаются 4 вопроса из разных тем курса. Студенту дается 30 минут на подготовку ответов. Затем студент озвучивает свои ответы.	В соответствии с пп. 2.5, 2.6 Положения

### 6.3. Оценочные материалы

Компетенции	Результаты обучения	№ КМ						
		1	2	3	4	5	6	7
ПК-6	Знает: стандарты в области управления рисками информационной безопасности	+	+	+	+	+	+	+
ПК-6	Умеет: применять программное обеспечение для оценки рисков информации безопасности	+	+	+	+	+	+	+
ПК-6	Имеет практический опыт: подбора инструментальных средств для управления информационными рисками			+	+	+	+	+

Фонды оценочных средств по каждому контрольному мероприятию находятся в приложениях.

## 7. Учебно-методическое и информационное обеспечение дисциплины

### Печатная учебно-методическая документация

*а) основная литература:*

Не предусмотрена

*б) дополнительная литература:*

1. Хашковский, А. В. Моделирование опасности. Анализ и оценка риска Учеб. пособие ЧГТУ, Каф. Безопасность жизнедеятельности. - Челябинск: Издательство ЧГТУ, 1995. - 31,[2] с. ил.

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

Не предусмотрены

*г) методические указания для студентов по освоению дисциплины:*

1. Учебное пособие (файл в приложении)

*из них: учебно-методическое обеспечение самостоятельной работы студента:*

1. Учебное пособие (файл в приложении)

### Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в	Библиографическое описание
---	----------------	------------------------	----------------------------

		электронной форме	
1	Основная литература	Электронно-библиотечная система издательства Лань	Основы информационной безопасности : учебное пособие / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. — Москва : Горячая линия-Телеком, 2011. — 558 с. — ISBN 5-93517-292-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <a href="https://e.lanbook.com/book/111016">https://e.lanbook.com/book/111016</a> (дата обращения: 10.11.2021). — Режим доступа: для авториз. пользователей.
2	Основная литература	Электронно-библиотечная система издательства Лань	Введение в информационную безопасность : учебное пособие / А. А. Малюк, В. С. Горбатов, В. И. Королев [и др.] ; под редакцией В. С. Горбатова. — Москва : Горячая линия-Телеком, 2018. — 288 с. — ISBN 978-5-9912-0160-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <a href="https://e.lanbook.com/book/111075">https://e.lanbook.com/book/111075</a> (дата обращения: 10.11.2021). — Режим доступа: для авториз. пользователей.
3	Дополнительная литература	Электронно-библиотечная система издательства Лань	Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : учебное пособие / П. Н. Девянин. — 2-е изд., испр. и доп. — Москва : Горячая линия-Телеком, 2017. — 338 с. — ISBN 978-5-9912-0328-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <a href="https://e.lanbook.com/book/111049">https://e.lanbook.com/book/111049</a> (дата обращения: 10.11.2021). — Режим доступа: для авториз. пользователей.

Перечень используемого программного обеспечения:

1. Microsoft-Office(бессрочно)
2. -Python(бессрочно)
3. Microsoft-Visual Studio(бессрочно)
4. Microsoft-Microsoft Imagine Premium (Windows Client, Windows Server, Visual Studio Professional, Visual Studio Premium, Windows Embedded, Visio, Project, OneNote, SQL Server, BizTalk Server, SharePoint Server)(04.08.2019)

Перечень используемых профессиональных баз данных и информационных справочных систем:

Нет

## 8. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Лабораторные занятия	333 (36)	Компьютеры, проектор, доска.