

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета  С.М. Пасмурнов
«31» августа 2017 г.



РАБОЧАЯ ПРОГРАММА

дисциплины

"Научно-исследовательская работа"

Специальность 10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Специализация Обеспечение информационной безопасности распределённых
информационных систем

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м. /-

Форма обучения очная/-

Год начала подготовки 2017

Автор программы

/Остапенко А.Г./

Заведующий кафедрой
Систем информационной
безопасности

/Остапенко А.Г./

Руководитель ОПОП

/Остапенко А.Г./

Воронеж 2017

1. ЦЕЛИ И ЗАДАЧИ ПРАКТИКИ

1.1. Цель практики подготовить аспиранта к профессиональной научно-исследовательской и преподавательской работе, основным результатом которой является получение и применения новых фундаментальных и прикладных результатов в области методов и систем защиты информации, информационной безопасности.

1.2. Задачи прохождения практики

- изучение теоретических основ закономерностей и тенденций в области методов и систем защиты информации, информационной безопасности;
- развитие способностей по разработке, развитию, использованию механизмов, модели и методов в области методов и систем защиты информации, информационной безопасности;
- овладение современными методами научно-исследовательской деятельности, как самостоятельно, так и в составе творческого коллектива с использованием современных информационно-коммуникационных технологий;
- совершенствование умений и навыков самостоятельной научно-исследовательской деятельности, овладение умениями изложения полученных результатов в виде отчетов, публикаций, докладов.

2. ХАРАКТЕРИСТИКА ПРАКТИКИ

Вид практики – Производственная практика

Тип практики – Научно-исследовательская работа

Форма проведения практики – дискретно

Способ проведения практики – стационарная, выездная.

Стационарная практика проводится в профильных организациях, расположенной на территории г. Воронежа.

Выездная практика проводится в местах проведения практик, расположенных вне г. Воронежа.

Способ проведения практики определяется индивидуально для каждого студента и указывается в приказе на практику.

Место проведения практики – перечень объектов для прохождения практик устанавливается на основе типовых двусторонних договоров между предприятиями (организациями) и ВУЗом или ВУЗ.

3. МЕСТО ПРАКТИКИ В СТРУКТУРЕ ОПОП

Практика «Научно-исследовательская работа» относится к базовой части блока Б2.

4. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПРИ ПРОХОЖДЕНИИ ПРАКТИКИ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс прохождения практики «Научно-исследовательская работа» направлен на формирование следующих компетенций:

ПК-1-способность осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке

ПК-2-способность создавать и исследовать модели автоматизированных систем

ПК-3-способность проводить анализ защищенности автоматизированных систем

ПК-4-способность разрабатывать модели угроз модели нарушителя информации безопасности автоматизированной системы

ПК-5-способность проводить анализ рисков информационной безопасности автоматизированной системы

ПК-6-способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности

ПК-8-способность разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем

ПК-10-способность применять знания в области электроники и схемотехники, технологий, методов языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности

ПК-12-способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы

ПК-13-способность участвовать в проектировании средств защиты информации автоматизированной системы

ПК-14-способность проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации

ПК-16-способность участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации

ПК-18-способность организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности

ПК-22-способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации

ПК-25-способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении штатных ситуаций

ПСК-7.1-способность разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз модели нарушителя

я информационной безопасности в распределенных информационных системах

ПСК-7.2-способностью проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах

ПСК-7.3-способностью проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем

ПСК-7.4-способностью проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах

ПСК-7.5-способностью координировать деятельность подразделений специалистов по защите информации в организациях, в том числе на предприятии и в учреждении

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ПК-1	Знать: Основные законы и понятия физики
	Уметь: находить закономерности при наблюдении и изучении физических явлений
	Владеть: навыком объяснения различных физических явлений.
ПК-2	Знать: основные методы исследования, используемые в физике.
	Уметь: проводить физико-математические и прикладные исследования.
	Владеть: способностью передавать результаты проведенных исследований в виде конкретных рекомендаций.
ПК-3	Знать: теоретические основы и базовые представления научного исследования в выбранной области фундаментальной или экспериментальной физики.
	Уметь: решать типичные задачи, формулировать выводы и приводить примеры, находить необходимые справочные материалы из информационных источников.
	Владеть: способностью проводить инструментальный мониторинг защищенности компьютерных систем.
ПК-4	Знать: методики анализа рисков, методы и средства управления информационными рисками.
	Уметь: разрабатывать корпоративную методику анализа рисков.
	Владеть: методами приближенного качественного описания физических процессов в изучаемых приборах,

	экспериментальными навыками для проведения научного исследования в избранной области физики.
ПК-5	Знать: нормативно-методические документы, описывающие методы анализа и исследований в области информационной безопасности.
	Уметь: применять знание физических теорий для анализа физических явлений.
	Владеть: Навыками использования информационных технологий для решения физических задач и применения численных методов.
ПК-6	Знать: основные свойства алгебраических структур.
	Уметь: уметь разрабатывать модели угроз информационной безопасности автоматизированной системы
	Владеть: Навыками использования современных информационных технологий для поиска, сбора, систематизации, обработки и интерпретации информации, необходимой для решения поставленных задач.
ПК-8	Знать: методики проверки работоспособности применяемых средств защиты.
	Уметь: проводить контрольные проверки работоспособности и эффективности применяемых криптографических средств защиты информации. проводить контрольные проверки работоспособности и эффективности применяемых технических средств защиты информации.
	Владеть: методиками построения линейных оптимальных систем управления информационной безопасностью компьютерной системы и их реализациями в современных инструментальных средах автоматизации инженерных и научных расчётов.

ПК-10	Знать: возможности технических средств перехвата информации.
	Уметь: Проводить мониторинг угроз безопасности компьютерных сетей.
	Владеть: Методами и средствами технической защиты информации.
ПК-12	Знать: терминологию , основные руководящие регламентирующие документы в области ЭВМ и систем, комплексов и систем.
	Уметь: Выполнять запрос к базе данных.
	Владеть: Навыками организации и обеспечения режима секретности.
ПК-13	Знать: Источники и классификацию угроз информационной безопасности.
	Уметь: Проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы.
	Владеть: Навыками анализа основных узлов и устройств современных автоматизированных системах.
ПК-14	Знать: основные понятия и последовательность этапов решения задачи оптимального управления необходимых для совершенствования системы управления информационной безопасностью компьютерной системы.
	Уметь: формализовать задачу управления безопасностью информационных систем, анализировать защищенность компьютерных систем.
	Владеть: методиками построения линейных оптимальных систем управления информационной безопасностью компьютерной системы и их реализациями в современных инструментальных средах автоматизации инженерных и научных расчётов.
ПК-16	Знать: Последовательность и содержание этапов построения компьютерных систем.
	Уметь: Восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем.
	Владеть: Методами расчёта и инструментального контроля показателей технической защиты

	информации.
ПК-18	Знать: Принципы построения и функционирования, примеры реализаций современных операционных систем. Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации
	Уметь: Использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем.
	Владеть: Навыками использования программно-аппаратных средств обеспечения безопасности компьютерных сетей
ПК-22	Знать: Основные методы управления информационной безопасностью.
	Уметь: Контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем.
	Владеть: Методами оценки информационных рисков. Навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем.
ПК-25	Знать: методики проверки работоспособности применяемых средств защиты
	Уметь: проводить контрольные проверки работоспособности и эффективности применяемых криптографических средств защиты информации. проводить контрольные проверки работоспособности и эффективности применяемых технических средств защиты информации
	Владеть: методиками построения линейных оптимальных систем управления информационной безопасностью компьютерной системы и их реализациями в современных инструментальных средах автоматизации инженерных и научных расчётов.
ПСК-7.1	Знать: характеристики основных каналов утечки информации на критически важных объектах.

	Уметь:составлять и оформлять акты контрольных проверок, анализировать результаты проверок и разрабатывать предложения по совершенствованию и повышению эффективности применения мер по технической защите информации на критически важных объектах.
	Владеть: навыками формулирования задач теоретической и прикладной физики.
ПСК-7.2	Знать: Способы обеспечения информационной безопасности систем организационного управления.
	Уметь: Разрабатывать модели систем организационного управления. Использовать технологии автоматизированного проектирования и структурный подход при проектировании информационных систем, определять ресурсы, необходимые для обеспечения безопасности информационной системы, использовать методы и средства определения технологической безопасности функционирования распределенной информационной системы.
	Владеть: Навыками разработки документации по метрологии, стандартизации и сертификации программных и аппаратных средств защиты.
ПСК-7.3	Знать: Специфику математического моделирования организационных задач в автоматизированных системах.
	Уметь:понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации .
	Владеть:навыками пользования нормативно правовыми актами в области технической защиты информации ограниченного доступа на предприятиях.
ПСК-7.4	Знать: Принципы построения распределённых систем и объектно-ориентированных систем управления базами данных, технологии автоматизированного проектирования баз данных.
	Уметь:организовывать защиту информации в

	распределённых компьютерных системах. Владеть: методами комплексного анализа для вычисления определённых и несобственных интегралов и решения других задач алгебры анализа.
ПСК-7.5	Знать: Нормативные документы по метрологии, стандартизации. Уметь: использовать современные программные средства для решения профессиональных задач. Владеть: навыком внедрения и использования системы мониторинга средств защиты информации, функционирующих на важных объектах.

5. ОБЪЕМ ПРАКТИКИ

Общий объем практики составляет 33 е.е., ее продолжительность – 2 недели.

Форма промежуточной аттестации: зачет с оценкой.

6. СОДЕРЖАНИЕ ПРАКТИКИ

6.1 Содержание разделов практики и распределение трудоемкости по этапам

№ п/п	Наименование этапа	Содержание этапа	Трудоемкость, час
1	Подготовительный этап	Проведение собрания по организации практики. Знакомство с целями, задачами, требованиями к практике и формой отчетности. Распределение заданий. Инструктаж по охране труда и пожарной безопасности.	2
2	Знакомство с ведущей организацией	Изучение организационной структуры организации. Изучение нормативно-технической документации.	10
3	Практическая работа	Выполнение индивидуальных заданий. Сбор практического материала.	84
4	Подготовка отчета	Обработка материалов практики, подбор и структурирование материала для раскрытия соответствующих тем для отчета. Оформление отчета. Предоставление отчета руководителю.	10
5	Защита отчета		2
Итого			108

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ПРОХОЖДЕНИЮ ПРАКТИКИ

7.1 Подготовка отчета о прохождении практики

Аттестация по итогам практики проводится в виде зачета с оценкой на основе экспертной оценки деятельности обучающегося за защиту отчета. По завершении практики студенты в последний день практики представляют на выпускающую кафедру: дневник практики, включающий всебя отзывы руководителей практики от предприятия и ВУЗа о работ студента в период практики с оценкой уровня оперативности выполнения им задания по практике, отношения к выполнению программ

ыпрактики и т.п.; отчет по практике, включающий текстовые, табличные и графические материалы, отражающие решение предусмотренных заданием на практику задач. В отчете приводится анализ поставленных задач; выбор необходимых методов и инструментальных средств для решения поставленных задач; результаты решения задач практики; общие выводы по практике. Типовая структура отчета:

1. Титульный лист
2. Содержание
3. Введение (цель практики, задачи практики)
4. Практические результаты прохождения практики
5. Заключение
6. Список использованных источников литературы
7. Приложения (при наличии)

7.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 8 семестре для очной формы обучения по четыре балльной системе:

- «отлично»;
 «хорошо»;
 «удовлетворительно»;
 «неудовлетворительно».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Экспертная оценка результатов	Отлично	Хорошо	Удовл.	Неудовл.
ПК-1	Знать: Основные законы и понятия физики	2 - полное освоение знания 1 – неполное освоение знания 0 – знание не освоено	Более 80% от максимального возможного количества баллов	61%-80% от максимального возможного количества баллов	41%-60% от максимального возможного количества баллов	Менее 41% от максимального возможного количества баллов
	Уметь: находить закономерности при наблюдении и изучении физических явлений	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умение не приобретено				
	Владеть: навыком объяснения различных физических явлений.	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владение не приобретено				
ПК-2	Знать: основные методы исследования, используемые в физике.	2 - полное освоение знания 1 – неполное освоение знания				

		0 – знание не освоено				
	Уметь: проводить физико-математические и прикладные исследования.	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умение не приобретено				
	Владеть: способностью передавать результаты проведенных исследований в виде конкретных рекомендаций.	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владение не приобретено				
ПК-3	Знать: теоретические основы и базовые представления научного исследования в выбранной области фундаментальной или экспериментальной физики.	2 - полное освоение знания 1 – неполное освоение знания 0 – знание не освоено				
	Уметь: решать типичные задачи, формулировать выводы и приводить примеры, находить необходимые справочные материалы из информационных источников.	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умение не приобретено				
	Владеть: способностью проводить инструментальный мониторинг защищенности компьютерных систем.	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владение не приобретено				
ПК-4	Знать: методики анализа рисков, методы и средства управления информационными рисками.	2 - полное освоение знания 1 – неполное освоение знания 0 – знание не освоено				
	Уметь: разрабатывать корпоративную методику анализа рисков.	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умение не приобретено				
	Владеть: методами приближенного	2 - полное приобретение				

	качественного описания физических процессов в изучаемых приборах, экспериментальными навыками для проведения научного исследования в избранной области физики.	е владения 1 – неполное приобретени е владения 0 – владение не приобретено				
ПК-5	Знать: нормативно-методические документы, описывающие методы анализа и исследований в области информационной безопасности.	2 - полное освоение знания 1 – неполное освоение знания 0 – знание не освоено				
	Уметь: применять знание физических теорий для анализа физических явлений.	2 - полное приобретени е умения 1 – неполное приобретени е умения 0 – умение не приобретено				
	Владеть: Навыками использования информационных технологий для решения физических задач и применения численных методов.	2 - полное приобретени е владения 1 – неполное приобретени е владения 0 – владение не приобретено				
ПК-6	Знать: основные свойства алгебраических структур.	2 - полное освоение знания 1 – неполное освоение знания 0 – знание не освоено				
	Уметь: уметь разрабатывать модели угроз информационной безопасности автоматизированной системы	2 - полное приобретени е умения 1 – неполное приобретени е умения 0 – умение не приобретено				
	Владеть: Навыками использования современных информационных технологий для поиска, сбора, систематизации, обработки и интерпретации информации, необходимой для решения поставленных задач.	2 - полное приобретени е владения 1 – неполное приобретени е владения 0 – владение не приобретено				

ПК-8	Знать: методики проверки работоспособности применяемых средств защиты.	2 - полное освоение знания 1 – неполное освоение знания 0 – знание не освоено				
	Уметь: проводить контрольные проверки работоспособности и эффективности применяемых криптографических средств защиты информации. проводить контрольные проверки работоспособности и эффективности применяемых технических средств защиты информации.	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умение не приобретено				
	Владеть: методиками построения линейных оптимальных систем управления информационной безопасностью компьютерной системы и их реализациями в современных инструментальных средах автоматизации инженерных и научных расчётов.	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владение не приобретено				
ПК-10	Знать: возможности технических средств перехвата информации.	2 - полное освоение знания 1 – неполное освоение знания 0 – знание не освоено				
	Уметь: Проводить мониторинг угроз безопасности компьютерных сетей.	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умение не приобретено				
	Владеть: Методами и средствами технической защиты информации.	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владение не приобретено				
ПК-12	Знать: терминологию ,	2 - полное				

	основные руководящие регламентирующие документы в области ЭВМ и систем, комплексов и систем.	освоение знания 1 – неполное освоение знания 0 – знание не освоено				
	Уметь: Выполнять запрос к базе данных.	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умение не приобретено				
	Владеть: Навыками организации и обеспечения режима секретности.	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владение не приобретено				
ПК-13	Знать: Источники и классификацию угроз информационной безопасности.	2 - полное освоение знания 1 – неполное освоение знания 0 – знание не освоено				
	Уметь: Проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы.	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умение не приобретено				
	Владеть: Навыками анализа основных узлов и устройств современных автоматизированных системах.	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владение не приобретено				
ПК-14	Знать: основные понятия и последовательность этапов решения задачи оптимального управления необходимых для совершенствования системы управления информационной безопасностью компьютерной системы.	2 - полное освоение знания 1 – неполное освоение знания 0 – знание не освоено				
	Знать: основные понятия и последовательность этапов решения задачи	2 - полное приобретение умения				

	оптимального управления необходимых для совершенствования системы управления информационной безопасностью компьютерной системы.	1 – неполное приобретение умения 0 – умение не приобретено				
	Владеть: методиками построения линейных оптимальных систем управления информационной безопасностью компьютерной системы и их реализациями в современных инструментальных средах автоматизации инженерных и научных расчётов.	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владение не приобретено				
ПК-16	Знать: Последовательность и содержание этапов построения компьютерных систем.	2 - полное освоение знания 1 – неполное освоение знания 0 – знание не освоено				
	Уметь: Восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем.	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умение не приобретено				
	Владеть: Методами расчёта и инструментального контроля показателей технической защиты информации.	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владение не приобретено				
ПК-18	Знать: Принципы построения и функционирования, примеры реализаций современных операционных систем. Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации	2 - полное освоение знания 1 – неполное освоение знания 0 – знание не освоено				
	Уметь: Использовать средства операционных систем для обеспечения эффективного и	2 - полное приобретение умения 1 – неполное				

	безопасного функционирования автоматизированных систем.	приобретение умения 0 – умение не приобретено				
	Владеть: Навыками использования программно-аппаратных средств обеспечения безопасности компьютерных сетей	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владение не приобретено				
ПК-22	Знать: Основные методы управления информационной безопасностью.	2 - полное освоение знания 1 – неполное освоение знания 0 – знание не освоено				
	Уметь: Контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем.	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умение не приобретено				
	Владеть: Методами оценки информационных рисков. Навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем.	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владение не приобретено				
ПК-25	Знать: методики проверки работоспособности применяемых средств защиты	2 - полное освоение знания 1 – неполное освоение знания 0 – знание не освоено				
	Уметь: проводить контрольные проверки работоспособности и эффективности применяемых криптографических средств защиты информации. проводить контрольные проверки работоспособности и эффективности применяемых технических средств защиты информации	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умение не приобретено				
	Владеть: методиками построения линейных	2 - полное приобретение				

	оптимальных систем управления информационной безопасностью компьютерной системы и их реализациями в современных инструментальных средах автоматизации инженерных и научных расчётов.	е владения 1 – неполное приобретени е владения 0 – владение не приобретено				
ПСК-7.1	Знать: Основные положения теории управления.	2 - полное освоение знания 1 – неполное освоение знания 0 – знание не освоено				
	Уметь: составлять и оформлять акты контрольных проверок, анализировать результаты проверок и разрабатывать предложения по совершенствованию и повышению эффективности применения мер по технической защите информации на критически важных объектах.	2 - полное приобретени е умения 1 – неполное приобретени е умения 0 – умение не приобретено				
	навыками формулирования задач теоретической и прикладной физики.	2 - полное приобретени е владения 1 – неполное приобретени е владения 0 – владение не приобретено				
ПСК-7.2	Знать: Способы обеспечения информационной безопасности систем организационного управления.	2 - полное освоение знания 1 – неполное освоение знания 0 – знание не освоено				
	Уметь: Разрабатывать модели систем организационного управления. Использовать технологии автоматизированного проектирования и структурный подход при проектировании информационных систем, определять ресурсы, необходимые для	2 - полное приобретени е умения 1 – неполное приобретени е умения 0 – умение не приобретено				

	обеспечения безопасности информационной системы, использовать методы и средства определения технологической безопасности функционирования распределенной информационной системы.					
	Владеть: Навыками разработки документации по метрологии, стандартизации и сертификации программных и аппаратных средств защиты.	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владение не приобретено				
ПСК-7.3	Знать: Специфику математического моделирования организационных задач в автоматизированных системах.	2 - полное освоение знания 1 – неполное освоение знания 0 – знание не освоено				
	Уметь: понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации .	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умение не приобретено				
	Владеть:навыками пользования нормативно правовыми актами в области технической защиты информации ограниченного доступа на предприятиях.	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владение не приобретено				
ПСК-7.4	Знать: Принципы построения распределённых систем и объектно-ориентированных систем управления базами данных, технологии автоматизированного проектирования баз данных.	2 - полное освоение знания 1 – неполное освоение знания 0 – знание не освоено				
	Уметь:организовывать защиту информации в распределённых компьютерных системах.	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умение не приобретено				
	Владеть:методами	2 - полное				

	комплексного анализа для вычисления определённых и несобственных интегралов и решения других задач алгебры анализа.	приобретение владения 1 – неполное приобретение владения 0 – владение не приобретено				
ПСК-7.5	Знать: Нормативные документы по метрологии, стандартизации.	2 - полное освоение знания 1 – неполное освоение знания 0 – знание не освоено				
	Уметь: использовать современные программные средства для решения профессиональных задач.	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умение не приобретено				
	навыком внедрения и использования системы мониторинга средств защиты информации, функционирующих на важных объектах.	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владение не приобретено				

Экспертная оценка результатов освоения компетенций производится руководителем практики (или согласованная оценка руководителя практики от ВУЗа и руководителя практики от организации).

8 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ПРАКТИКИ

8.1 Перечень учебной литературы, необходимой для освоения практик

и

Основная литература

1. Эпидемии в телекоммуникационных сетях [Текст] / под ред. Д. А. Новикова. - Москва : Горячая линия - Телеком, 2018. - 282 с. : ил. - (Теория сетевых войн. № 1). - Библиогр.: с. 231-245 (244 назв.). - ISBN 978-5-9912-0682-2 : 736-00.

2. Социальные сети и деструктивный контент [Текст] / под ред. Д. А. Новикова. - Москва : Горячая линия - Телеком, 2018. - 274 с. : ил. - (Теория сетевых войн. № 3). - Библиогр.: с. 224-239 (278 назв.). - ISBN 978-5-9912-0686-0 : 719-00.

3. Атакуемые взвешенные сети [Текст] / под ред. Д. А. Новикова. - Москва : Горячая линия - Телеком, 2018. - 247 с. : ил. - (Теория сетевых войн. № 2). - Библиогр.: с. 201-213 (214 назв.). - ISBN 978-5-9912-0684-6 : 708-00.

Дополнительная литература

1. Теория сетевых войн [Электронный ресурс] : Учеб. пособие. - Электрон. текстовые, граф. дан. (894 Мб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 30-00.
2. Сетевое противоборство социотехнических систем [Электронный ресурс] . - Электрон. текстовые, граф. дан. (474 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 30-00.
3. Информационные технологии и системы государственного и муниципального управления [Электронный ресурс] : учеб. пособие. - Электрон. дан. (1 файл : 3164 Кб). - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2007. - 1 файл. - 30-00.

8.2 Перечень ресурсов сети "Интернет", необходимых для проведения практики

<http://att.nica.ru>
<http://www.edu.ru/>
<http://window.edu.ru/window/library>
<http://www.intuit.ru/catalog/>
<https://marsohod.org/howtostart/marsohod2>
<http://bibl.cchgeu.ru/MarcWeb2/ExtSearch.asp>
<https://cchgeu.ru/education/cafedras/kafsib/?docs>
<http://www.eios.vorstu.ru>
<http://e.lanbook.com/> (ЭБС Лань)
<http://IPRbookshop.ru/> (ЭБС IPRbooks)

8.3 Перечень информационных технологий, используемых при осуществлении образовательного процесса по практике, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

1. Microsoft Office Excel 2013/2007 (Контракт №72, 12.12.2014)
2. Microsoft Office Word 2013/2007 (Контракт №72, 12.12.2014)
3. Интегрированная среда разработки для языка программирования R (GNU GPLv2)
4. Программный комплекс «Netepidemic» для риск-анализа процессов распространения деструктивного контента в неоднородных сетевых структурах.

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ

Специализированная лекционная аудитория, оснащенная оборудованием для лекционных демонстраций и проекционной аппаратурой.