МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ 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 ПРАКТИКИ

«Научно-исследовательская работа»

Специальность 10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Специализация

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет

Форма обучения очная

Год начала подготовки 2016

Автор программы _____ / А.Г. Остапенко /

Заведующий кафедрой
Систем информационной
безопасности _____ / А.Г. Остапенко /

Руководитель ОПОП _____ / А.Г. Остапенко /

Воронеж 2017

1.ЦЕЛИИЗАДАЧИПРАКТИКИ

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.Задачипрохожденияпрактики

- 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.ХАРАКТЕРИСТИКАПРАКТИКИ

Видпрактики–Производственнаяпрактика

Типпрактика–Научно-исследовательскаяработа

Формапроведенияпрактики–дискретно

Способпроведенияпрактики–стационарная,выездная.

Стационарнаяпрактикапроводитсявпрофильныхорганизациях,расположеннойнатерриторииг.Воронежа.

Выезднаяпрактикапроводитсявместахпроведенияпрактик,расположенныхвнег.Воронежа.

Способпроведенияпрактикиопределяетсяиндивидуальнодлякаждогостудентаиуказываетсявприказенапрактику.

Местопроведенияпрактики–переченьобъектовдляпрохожденияпрактикиустанавливаетсянаосноветиповыхдвусторонних договоровмеждупредприятиями(организациями)иВУЗомилиВУЗ.

3.МЕСТОПРАКТИКИВСТРУКТУРЕОПОП

Практика«Научно-исследовательскаяработа»относитсякбазовойчастиблокаБ2.

4.ПЕРЕЧЕНЬПЛАНИРУЕМЫХРЕЗУЛЬТАТОВОБУЧЕНИЯПРИПРОХОЖДЕНИИПРАКТИКИ,СООТНЕСЕННЫХСПЛАНИРУЕМЫМИРЕЗУЛЬТАТАМИОСВОЕНИЯОБРАЗОВАТЕЛЬНОЙПРОГРАММЫ

Процесспрохожденияпрактики«Научно-исследовательскаяработа»направленаформированиеследующихкомпетенций:

ПК-1-способностьюосуществлятьпоиск,изучение,обобщениеисистематизациюнаучно-техническойинформации,нормативныхиметодическихматериаловвсферепрофессиональнойдеятельности,втомчисленаиностранномязыке;

ПК-2-способностьюсоздаватьиисследоватьмоделиавтоматизированныхсистем;

ПК-3-способностьюпроводитьанализзащищенностиавтоматизированныхсистем;

ПК-4-способностьюразрабатыватьмоделиугрозимоделинарушителяинформационнойбезопасностиавтоматизированнойсистемы;

ПК-5-способностьюпроводитьанализрисковинформационнойбезопасностиавтоматизированнойсистемы;

ПК-6-способностьюпроводитьанализ,предлагатьиобосновыватьвыборрешенийпообеспечениюэффективногоприменения автоматизированныхсистемвсферепрофессиональнойдеятельности;

ПК-8-способностьюразрабатыватьианализироватьпроектныерешенияпообеспечениюбезопасностиавтоматизированныхсистем;

ПК-10-способностьюприменятьзнаниявобластиэлектроникиисхемотехники,технологий,методовиязыковпрограммирования,технологийсвязииередачиданныхприразработкепрограммно-аппаратныхкомпонентовзащищенныхавтоматизированныхсистемвсферепрофессиональнойдеятельности;

ПК-12-способностьюучаствоватьвпроектированиисистемыуправленияинформационнойбезопасностьюавтоматизированнойсистемы;

ПК-13-способностьюучаствоватьвпроектированиисредствзащитыинформацииавтоматизированнойсистемы;

ПК-14-способностьюпроводитьконтрольныепроверкиработоспособноститиприменяемыхпрограммно-аппаратных,криптографическихитехническихсредствзащитыинформации;

ПК-16-способностьюучаствоватьвпроведенииэкспериментально-исследовательскихработприаттестацииавтоматизированныхсистемсучетомнормативныхдокументовпозащитеинформации;

ПК-18-способностьюорганизовыватьработумалыхколлективовисполнителей,вырабатыватьиреализовыватьуправленческиерешениявсферепрофессиональнойдеятельности;

ПК-22-способностьюучаствоватьвформированииполитикиинформационнойбезопасностиорганизацииконтролироватьэффективностьеереализации;

ПК-25-способностьюобеспечитьэффективноеприменениесредствзащитыинформационно-технологическихресурсовавтоматизированнойсистемыивосстановлениеихработоспособностипривозникновенииинештатныхситуаций;

ПСК-7.1-способностьразрабатыватьиисследоватьмоделиинформационно-технологическихресурсов,разрабатыватьмоделиугрозимоделинарушителяи

нформационнойбезопасностивраспределенныхинформационныхсистемах;

ПСК-7.2-способностьюпроводитьанализрисковинформационнойбезопасностииразрабатывать,руководитьразработкойполитикибезопасностивраспределенныхинформационныхсистемах;

ПСК-7.3-способностьюпроводитьаудитзащищенностиинформационно-технологическихресурсовраспределенныхинформационныхсистем;

ПСК-7.4-способностьюпроводитьудаленноеадминистрированиеоперационныхсистемисистембазданныхвраспределенныхинформационныхсистемах;

ПСК-7.5-способностьюкоординироватьдеятельностьподразделенийспециалистовпозащитеинформацииворганизациях,втомчисленапредприятииивучреждении

Компетенция	**Результатыобучения,характеризующие сформированностькомпетенции**
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 результата 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

Общийобъемпрактикисоставляетсоставляет3з.е.,еепродолжительность –2недели.

Формапромежуточнойаттестации:зачетсоценкой.

6.СОДЕРЖАНИЕПРАКТИКИ

6.1Содержаниеразделовпрактикииираспределениетрудоемкостипоэтапам

№ 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.ОЦЕНОЧНЫЕМАТЕРИАЛЫДЛЯПРОВЕДЕНИЯПРОМЕЖУТОЧНОЙАТТЕСТАЦИИПОПРОХОЖДЕНИЮПРАКТИКИ

7.1Подготовкаотчетаопрохожденииипрактики

Аттестацияпоитогампрактикипроводитсяввидезачетасоценкойнаосновеэкспертнойоценкидеятельностиобучающегосяизащитыотчета.Позавершениипрактикистудентывпоследнийденьпрактикипредставляютнавыпускающуюкафедру:дневникпрактики,включающийвсебяотзывыруководителейпрактикиотпредприятияиВУЗаоработестудентавпериодпрактикисоценкойуровняиоперат

ивностивыполненияимзаданияпопрактике,отношенияквыполнениюпрограммыпрактикиит.п.;отчетпопрактике,включающийтекстовые,табличныеиграфическиематериалы,отражающиерешениепредусмотренныхзаданиемнапрактикузадач.Вотчетеприводитсяанализпоставленныхзадач;выборнеобходимыхметодовиинструментальныхсредствдлярешенияпоставленныхзадач;результатырешениязадачпрактики;общиевыводыпопрактике.Типоваяструктураотчета:

1.Титульныйлист
2.Содержание
3.Введение(цельпрактики,задачипрактики)
4.Практическиерезультатыпрохожденияпрактики
5.Заключение
6.Списокиспользованныхисточниковилитературы
7.Приложения(приналичии)

7.2Этаппромежуточногоконтролязнаний

Результатыпромежуточногоконтролязнанийоцениваютсяв8семестредля очнойформыобученияпочетырехбалльнойсистеме:

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

Компе-тенция	**Результатыобучения,характеризующие сформированностькомпетенции**	**Экспертная оценкарезультатов**	**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 максимальн о возможного количества баллов	61%-80% от максимальн о возможного количества баллов	41%-60% от максимально возможного количества баллов	Менее 41% от максимальн о возможног о количества баллов
	Уметь: находить закономерности при наблюдении и изучении физических явлений	2 - полное приобретени е умения 1 – неполное приобретени е умения 0 – умение не приобретено				
	Владеть:навыком объяснения различных физических явлений.	2 - полное приобретени е владения 1 – неполное приобретени е 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 результата 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	2 - полное				

	приближенного качественного описания физических процессов в изучаемых приборах, экспериментальными навыками для проведения научного исследования в избранной области физики.	приобретение владения 1 – неполное приобретение 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 приобретение умения 1 – неполное приобретение умения 0 – умение не приобретено				
	Владеть: Навыками использования информационных технологий для решения физических задач и применения численных методов.	2 - полное приобретение владения 1 – неполное приобретение 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 приобретение умения 1 – неполное приобретение умения 0 – умение не приобретено				
	Владеть: Навыками использования современных информационных технологий для поиска, сбора, систематизации, обработки и интерпретации информации, необходимой для решения	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владение не приобретено				

	поставленных задач.					
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 , основные руководящие регламентирующие документы в области ЭВМ и систем, комплексов и систем.	2 - полное 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	2 - полное приобретени				

	решения задачи оптимального управления необходимых для совершенствования системы управления информационной безопасностью компьютерной системы.	е умения 1 – неполное приобретени е 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 приобретени е владения 1 – неполное приобретени е 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 приобретени е умения 1 – неполное приобретени е умения 0 – умение не приобретено				
	Владеть: Методами расчёта и инструментального контроля показателей технической защиты информации.	2 - полное приобретени е владения 1 – неполное приобретени е 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	2 - полное приобретени е умения				

	эффективного и безопасного функционирования автоматизированных систем.	1 – неполное 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	2 - полное				

	построения линейных оптимальных систем управления информационной безопасностью компьютерной системы и их реализациями в современных инструментальных средах автоматизации инженерных и научных расчётов.	приобретение владения 1 – неполное приобретение 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 приобретение умения 1 – неполное приобретение умения 0 – умение не приобретено				
	навыками формулирования задач теоретической и прикладной физики.	2 - полное приобретение владения 1 – неполное приобретение 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,	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умение не приобретено				

	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.	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 комплексного анализа для вычисления определённых и несобственных интегралов и решения других задач алгебры анализа.	2 - полное 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				

Экспертнаяоценкарезультатовосвоениякомпетенцийпроизводитсяруководителемпрактики(илисогласованнаяоценкаруководителяпрактикиотВУЗаируководителяпрактикиоторганизации).

8УЧЕБНО-МЕТОДИЧЕСКОЕИИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕПРАКТИКИ

8.1Переченьучебнойлитературы,необходимойдляосвоенияпрактики

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.

8.2Переченьресурсовсети"Интернет",необходимыхдляпроведения 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/ (ЭБСIPRbooks)

8.3Переченьинформационныхтехнологий,используемыхприосуществлениииобразовательногопроцессапопрактике,включаяпереченьлицензионногопрограммногообеспечения,ресурсовинформационно-телекоммуникационнойсети«Интернет»,современныхпрофессиональныхбазданныхиинформационныхсправочныхсистем:

1.Microsoft Office Excel 2013/2007 (Контракт №72, 12.12.2014)

2. MicrosoftOfficeWord 2013/2007 (Контракт №72, 12.12.2014)

3. Интегрированная среда разработки для языка программирования R (GNUGPLv2)

4. Программный комплекс «Netepidemic» для риск-анализа процессов распространения деструктивного контента в неоднородных сетевых структурах.

9МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯБАЗА,НЕОБХОДИМАЯДЛЯПРОВЕДЕНИЯПРАКТИКИ

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