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

«Преддипломная практика»

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.Целипрактики

Производственная практика (преддипломная) студентов является заключительной частью образовательного процесса и направлена на закрепление и углубление компетенций, полученных студентами в процессе всего предыдущего обучения, а также на углубление студентом первоначального профессионального опыта, развитие общих и профессиональных компетенцийи опытомпрофессиональной деятельности по получаемой специальности.

1.2.Задачипрохожденияпрактики

1)Обобщение и совершенствование знаний и практических навыков, полученных студентамив процессе обучения по специальности;

2)Проверка возможностей самостоятельной работы будущего специалиста в условиях конкретного производства;

3)Сбор материала для выполнения дипломного проекта;

2.ХАРАКТЕРИСТИКАПРАКТИКИ

Видпрактики–Производственнаяпрактика

Типпрактика–Преддипломнаяпрактика

Формапроведенияпрактики–дискретно

Способпроведенияпрактики–стационарная,выездная.

Стационарнаяпрактикапроводитсявпрофильныхорганизациях,расположеннойнатерриторииг.Воронежа.

Выезднаяпрактикапроводитсявместахпроведенияпрактик,расположенныхвнег.Воронежа.

Способпроведенияпрактикиопределяетсяиндивидуальнодлякаждогостудентаиуказываетсявприказенапрактику.

Местопроведенияпрактики–переченьобъектовдляпрохожденияпрактикиустанавливаетсянаосноветиповыхдвусторонних договоровмеждупредприятиями(организациями)иВУЗомилиВУЗ.

3.МЕСТОПРАКТИКИВСТРУКТУРЕОПОП

Практика«Преддипломнаяпрактика»относитсякбазовойчастиблока Б2.

4.ПЕРЕЧЕНЬПЛАНИРУЕМЫХРЕЗУЛЬТАТОВОБУЧЕНИЯПРИПРОХОЖДЕНИИПРАКТИКИ,СООТНЕСЕННЫХСПЛАНИРУЕМЫМИРЕЗУЛЬТАТАМИОСВОЕНИЯОБРАЗОВАТЕЛЬНОЙПРОГРАММЫ

Процесспрохожденияпрактики«Преддипломнаяпрактика»направленна формированиеследующихкомпетенций:

ОПК-1-способностьюанализироватьфизическиеявленияипроцессы,применятьсоответствующийматематическийаппаратдляформализацииирешенияпрофессиональныхзадач;

ОПК-2-способностьюкорректноприменятьприрешенииипрофессиональныхзадачсоответствующийматематическийаппараталгебры,геометрии,дискретнойматематики,математическогоанализа,теорииверо ятностей,математическо

йстатистики,математическойлогики,теорииалгоритмов,теорииинформации,втомчислесиспользованиемвычислительнойтехники;

ОПК-3-способностьюприменятьязыки,системыиинструментальныесредствапрограммированиявпрофессиональнойдеятельности;

ОПК-4-способностьюпониматьзначениеинформациивразвитиисовременногообщества,применятьдостижениясовременныхинформационныхтехнологийдляпоискаинформациивкомпьютерныхсистемах,сетях,библиотечныхфондах;

ОПК-5-способностьюприменятьметодынаучныхисследованийвпрофессиональнойдеятельности,втомчислевработенадмеждисциплинарнымииинновационнымипроектами;

ПК-4-способностьюразрабатыватьмоделиугрозимоделинарушителяинформационнойбезопасностиавтоматизированнойсистемы;

ПК-7-способностьюразрабатыватьнаучно-техническуюдокументацию,готовитьнаучно-техническиеотчеты,обзоры,публикациипорезультатамвыполненныхработ;

ПК-19-способностьюразрабатыватьпредложенияпосовершенствованию системыуправленияинформационнойбезопасностьюавтоматизированнойсистемы;

ПК-21-способностьюразрабатыватьпроектыдокументов,регламентирующихработупообеспечениюинформационнойбезопасностиавтоматизированныхсистем;

ПК-22-способностьюучаствоватьвформированииполитикиинформационнойбезопасностиорганизацииконтролироватьэффективностьеереализации;

ПК-25-способностьюобеспечитьэффективноеприменениесредствзащитыинформационно-технологическихресурсовавтоматизированнойсистемыивосстановлениеихработоспособностипривозникновенииинештатныхситуаций;

ПК-26-способностьюадминистрироватьподсистемуинформационнойбезопасностиавтоматизированнойсистемы;

ПК-27-способностьювыполнятьполныйобъемработ,связанныхсреализациейчастныхполитикинформационнойбезопасностиавтоматизированнойсистемы,осуществлятьмониторингиаудитбезопасностиавтоматизированнойсистемы;

ПК-28-способностьюуправлятьинформационнойбезопасностьюавтоматизированнойсистемы;

ПСК-7.1-способностьразрабатыватьиисследоватьмоделиинформационно-технологическихресурсов,разрабатыватьмоделиугрозимоделинарушителяинформационнойбезопасностивраспределенныхинформационныхсистемах;

ПСК-7.2-способностьюпроводитьанализрисковинформационнойбезопасностииразрабатывать,руководитьразработкойполитикибезопасностивраспределенныхинформационныхсистемах;

ПСК-7.3-способностьюпроводитьаудитзащищенностиинформационно-технологическихресурсоврапределенныхинформационныхсистем;

ПСК-7.4-способностьюпроводитьудаленноеадминистрированиеоперационныхсистемисистембазданныхвраспределенныхинформационныхсистемах

;

ПСК-7.5-способностьюкоординироватьдеятельностьподразделенийисп
ециалистовпозащитеинформацииворганизациях,втомчисленапредприятииив
чреждении

Компетенция	**Результатыобучения,характеризующие сформированностькомпетенции**
ОПК-1	Знать теоретические основы и задачи физики и математики в контексте обеспечения информационной безопасности автоматизированных систем
	Уметь определять возможности применения на практике физико-математических теоретических положений и методов для постановки и решения прикладных задач по защите информации
	Владеть моделями и методиками физико-математического моделирования процессов нарушения информационной безопасности в автоматизированных систем
ОПК-2	Знать теоретические основы алгебры, геометрии, математического анализа, теории вероятности, математической статистики, математической логики, теории алгоритмов, теории информации в контексте обеспечения информационной безопасности автоматизированных систем
	Уметь применять на практике математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятности, математической статистики, теории алгоритмов, теории информации для решения практических задач в контексте информационной безопасности автоматизированных систем
	Владеть методами математического исследования процессов нарушения информационной безопасности автоматизированных систем
ОПК-3	Знать современные теоретические и технические основы программирования
	Уметь применять на практике навыки прикладного программирования для решения профессиональных задач в области обеспечения информационной безопасности

	автоматизированных систем
	Владеть языками и методами программирования в целях обеспечения безопасности автоматизированных систем
ОПК-4	Знать теоретические и практические возможности современных информационных технологий для развития общества
	Уметь применять достижения современных информационных технологий для поиска, хранения, обработки информации
	Владеть навыками работы с современными технологическими инструментами в инфокоммуникационной сфере
ОПК-5	Знать методы научных исследований в профессиональной деятельности
	Уметь применять теоретическую базу для проектирования программного обеспечения и устройств
	Владеть навыками и методами создания программного обеспечения и устройств для решения профессиональных задач
ПК-4	Знать теоретические основы моделирования угроз и нарушителей информационной безопасности автоматизированных систем
	Уметь разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем
	Владеть приемами практического применения моделей угроз и нарушителей информационной безопасности автоматизированных систем
ПК-7	Знать основы работы с научно-технической документацией
	Уметь готовить научно-технические отчеты, обзоры и публикации по результатам выполненных работ
	Владеть навыками компьютерной работы с научно-технической документацией, публикацией статей и монографий
ПК-19	Знать принципы организации системы управления информационной безопасностью автоматизированных систем
	Уметь разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности

	автоматизированных систем
	Владеть инструментарием оценки защищенности автоматизированных систем
ПК-21	Знать теоретические и правовые основы разработки проектов документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем
	Уметь разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем
	Владеть навыками разработки документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем
ПК-22	Знать принципы формирования политики обеспечения информационной безопасности автоматизированных систем
	Уметь формулировать цели и задачи обеспечения информационной безопасности автоматизированных систем
	Владеть навыками контроля эффективности обеспечения информационной безопасности автоматизированных систем
ПК-25	Знать классификацию средств защиты информационно-технологическихресурсовавтоматизированнойсистемы и теоретические и технические основы их применения
	Уметь на практике применять средствазащитыинформационно-технологическихресурсовавтоматизированнойсистемыивосстанавливатьихработоспособностипривозникновениинештатныхситуаций
	Владеть навыками эффективного применения комплекса средствзащитыинформационно-технологическихресурсовавтоматизированнойсистемыивосстановлениеихработоспособностипривозникновениинештатныхситуаций для решения профессиональных задач
ПК-26	Знать основы администрирования процессов обеспечения информационной безопасности автоматизированных систем

	Уметь применять принципы администрирования систем информационной безопасности в конкретных организационно-правовых направлениях обеспечения безопасности автоматизированных систем
	Владеть методами и средствами администрирования систем обеспечения информационной безопасности автоматизированных систем
ПК-27	Знать принципы контроля основных параметров подсистем обеспечения информационной безопасности автоматизированных систем
	Уметь применять на практике методики мониторинга и аудита обеспечения информационной безопасности автоматизированных систем
	Владеть техникой обработки результатов мониторинга и аудита обеспечения информационной безопасности автоматизированных систем
ПК-28	Знать теоретические и технические основы управления информационной безопасностью автоматизированных систем
	Уметь решать задачи, связанные с управлением информационной безопасностью автоматизированных систем
	Владеть приемами эффективного управления информационной безопасностью автоматизированных систем
ПСК-7.1	Знать теоретические основы моделирования угроз и нарушителей информационной безопасности автоматизированных систем
	Уметь разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем
	Владеть приемами практического применения моделей угроз и нарушителей информационной безопасности автоматизированных систем
ПСК-7.2	Знать теоретические основы риск-анализа информационной безопасности автоматизированных систем
	Уметь применять на практике методы оценки

	ущербов и вероятности их наступления в условиях нарушения информационной безопасности автоматизированных систем
	Владеть навыками комплексной оценки рисков и защищенности автоматизированных систем
ПСК-7.3	Знать принципы организации аудита защищенности ресурсов распределенных информационных систем
	Уметь применять на практике приемы и средства аудита защищенности информационно-технологических ресурсов распределенных информационных систем
	Владеть навыками проведения комплексного аудита и выработки предложений по усовершенствованию политики защиты информационно-технологических ресурсов распределенных информационных систем
ПСК-7.4	Знать принципы организации удаленного администрирования операционных систем и систем баз данных в распределенных информационных системах
	Уметь организовывать на практике удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах
	Владеть навыками комплексного администрирования операционных систем и баз данных распределенных информационных систем
ПСК-7.5	Знать теоретические основы организационного управления в области обеспечения информационной безопасности автоматизированных систем
	Уметь координировать деятельность подразделений и специалистов в отдельно взятой организации
	Владеть навыками комплексной оценки эффективности деятельности подразделений и специалистов по защите информации в организациях

5. ОБЪЕМ ПРАКТИКИ

Общийобъемпрактикисоставляетсоставляет18з.е.,еепродолжительность–12недель.

Формапромежуточнойаттестации:зачетсоценкой.

6.СОДЕРЖАНИЕПРАКТИКИ

6.1Содержаниеразделовпрактикииираспределениетрудоемкостипоэтапам

№ п/п	Наименованиеэтапа	Содержаниеэтапа	Трудоемкость, час
1	Подготовительныйэтап	Проведение собрания по организации практики. Знакомство с целями, задачами, требованиями к практике и формой отчетности. Распределениезаданий. Инструктажпоохранетруда и пожарнойбезопасности.	*2*
2	Знакомство с ведущейорганизацией	Изучение организационной структуры организации. Изучение нормативно-технической документации.	*10*
3	Практическаяработа	Выполнение индивидуальных заданий. Сбор практического материала.	*624*
4	Подготовкаотчета	Обработка материалов практики, подбор и структурирование материала для раскрытия соответствующих тем для отчета. Оформлениеотчета. Предоставлениеотчетаруководителю.	*10*
5	Защитаотчета		*2*
		Итого	*648*

7.ОЦЕНОЧНЫЕМАТЕРИАЛЫДЛЯПРОВЕДЕНИЯПРОМЕЖУТОЧНОЙАТТЕСТАЦИИПОПРОХОЖДЕНИЮПРАКТИКИ

7.1Подготовкаотчетаопрохожденииипрактики

Аттестацияпоитогампрактикипроводитсяввидезачетасоценкойнаосновеэкспертнойоценкидеятельностиобучающегосяизащитыотчета.Позавершениипрактикистудентывпоследнийденьпрактикипредставляютнавыпускающуюкафедру:дневникпрактики,включающийвсебяотзывыруководителейпрактикиотпредприятияиВУЗаоработестудентавпериодпрактикисоценкойуровняоперативностивыполненияимзаданияпопрактике,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

Результатыпромежуточногоконтролязнанийоцениваютсяв10семестред

ляочнойформыобученияпочетырехбалльнойсистеме:

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

Компе-тенция	Результатыобучения,характеризующие сформированностькомпетенции	Экспертная оценкарезультатов	Отлично	Хорошо	Удовл.	Неудовл.
ОПК-1	Знать теоретические основы и задачи физики и математики в контексте обеспечения информационной безопасности автоматизированных систем	2 - полное освоение знания 1 – неполное освоение знания 0 – знаниенеосвоено	Более 80% от максимального возможного количества баллов	61%-80% от максимального возможного количества баллов	41%-60% от максимально возможного количества баллов	Менее 41% от максимальн о возможного количества баллов
	Уметь определять возможности применения на практике физико-математических теоретических положений и методов для постановки и решения прикладных задач по защите информации	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умениенеприобретено				
	Владеть моделями и методиками физико-математического моделирования процессов нарушения информационной безопасности в автоматизированных систем	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владениенеприобретено				
ОПК-2	Знать теоретические основы алгебры, геометрии, математического анализа, теории вероятности, математической статистики, математической логики, теории алгоритмов, теории информации в контексте обеспечения информационной безопасности автоматизированных систем	2 - полное освоение знания 1 – неполное освоение знания 0 – знаниенеосвоено				
	Уметь применять на практике математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятности, математической статистики, теории алгоритмов, теории информации для решения практических задач в контексте информационной безопасности автоматизированных систем	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умениенеприобретено				

	Владеть методами математического исследования процессов нарушения информационной безопасности автоматизированных систем	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владениенеприобретено				
ОПК-3	Знать современные теоретические и технические основы программирования	2 - полное освоение знания 1 – неполное освоение знания 0 – знаниенеосвоено				
	Уметь применять на практике навыки прикладного программирования для решения профессиональных задач в области обеспечения информационной безопасности автоматизированных систем	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умениенеприобретено				
	Владеть языками и методами программирования в целях обеспечения безопасности автоматизированных систем	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владениенеприобретено				
ОПК-4	Знать теоретические и практические возможности современных информационных технологий для развития общества	2 - полное освоение знания 1 – неполное освоение знания 0 – знаниенеосвоено				
	Уметь применять достижения современных информационных технологий для поиска, хранения, обработки информации	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умениенеприобретено				
	Владеть навыками работы с современными технологическими инструментами в инфокоммуникационной сфере	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владениенеп				

		риобретено				
ОПК-5	Знать методы научных исследований в профессиональной деятельности	2 - полное освоение знания 1 – неполное освоение знания 0 – знаниенеосвоено				
	Уметь применять теоретическую базу для проектирования программного обеспечения и устройств	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умениенеприобретено				
	Владеть навыками и методами создания программного обеспечения и устройств для решения профессиональных задач	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владениенеприобретено				
ПК-4	Знать теоретические основы моделирования угроз и нарушителей информационной безопасности автоматизированных систем	2 - полное освоение знания 1 – неполное освоение знания 0 – знаниенеосвоено				
	Уметь разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умениенеприобретено				
	Владеть приемами практического применения моделей угроз и нарушителей информационной безопасности автоматизированных систем	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владениенеприобретено				
ПК-7	Знать основы работы с научно-технической документацией	2 - полное освоение знания 1 – неполное освоение знания 0 –				

		знаниенеосвоено				
	Уметь готовить научно-технические отчеты, обзоры и публикации по результатам выполненных работ	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умение не приобретено				
	Владеть навыками компьютерной работы с научно-технической документацией, публикацией статей и монографий	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владениенеприобретено				
ПК-19	Знать принципы организации системы управления информационной безопасностью автоматизированных систем	2 - полное освоение знания 1 – неполное освоение знания 0 – знаниенеосвоено				
	Уметь разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умениенеприобретено				
	Владеть инструментарием оценки защищенности автоматизированных систем	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владениенеприобретено				
ПК-21	Знать теоретические и правовые основы разработки проектов документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	2 - полное освоение знания 1 – неполное освоение знания 0 – знаниенеосвоено				
	Уметь разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной	2 - полное приобретение умения 1 – неполное приобретение умения				

	безопасности автоматизированных систем	0 – умениенеприобретено				
	Владеть навыками разработки документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владениенеприобретено				
ПК-22	Знать принципы формирования политики обеспечения информационной безопасности автоматизированных систем	2 - полное освоение знания 1 – неполное освоение знания 0 – знаниенеосвоено				
	Уметь формулировать цели и задачи обеспечения информационной безопасности автоматизированных систем	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умениенеприобретено				
	Владеть навыками контроля эффективности обеспечения информационной безопасности автоматизированных систем	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владениенеприобретено				
ПК-25	Знать классификацию средств защиты информационно-технологических ресурсов автоматизированной системы и теоретические и технические основы их применения	2 - полное освоение знания 1 – неполное освоение знания 0 – знаниенеосвоено				
	Уметь на практике применять средства защиты информационно-технологических ресурсов автоматизированной системы и восстанавливать их работоспособности при возникновении нештатных ситуаций	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умениенеприобретено				
	Владеть навыками эффективного применения комплекса средств защиты информационно-технологических ресурсов	2 - полное приобретение владения 1 – неполное приобретени				

	автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций для решения профессиональных задач	е владения 0 – владениенеприобретено				
ПК-26	Знать основы администрирования процессов обеспечения информационной безопасности автоматизированных систем	2 - полное освоение знания 1 – неполное освоение знания 0 – знаниенеосвоено				
	Уметь применять принципы администрирования систем информационной безопасности в конкретных организационно-правовых направлениях обеспечения безопасности автоматизированных систем	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умениенеприобретено				
	Владеть методами и средствами администрирования систем обеспечения информационной безопасности автоматизированных систем	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владениенеприобретено				
ПК-27	Знать принципы контроля основных параметров подсистем обеспечения информационной безопасности автоматизированных систем	2 - полное освоение знания 1 – неполное освоение знания 0 – знаниенеосвоено				
	Уметь применять на практике методики мониторинга и аудита обеспечения информационной безопасности автоматизированных систем	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умениенеприобретено				
	Владеть техникой обработки результатов мониторинга и аудита обеспечения информационной безопасности автоматизированных систем	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владениенеприобретено				
ПК-28	Знать теоретические и технические основы	2 - полное освоение				

	управления информационной безопасностью автоматизированных систем	знания 1 – неполное освоение знания 0 – знаниенеосвоено				
	Уметь решать задачи, связанные с управлением информационной безопасностью автоматизированных систем	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умениенеприобретено				
	Владеть приемами эффективного управления информационной безопасностью автоматизированных систем	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владениенеприобретено				
ПСК-7.1	Знать теоретические основы моделирования угроз и нарушителей информационной безопасности автоматизированных систем	2 - полное освоение знания 1 – неполное освоение знания 0 – знаниенеосвоено				
	Уметь разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умениенеприобретено				
	Владеть приемами практического применения моделей угроз и нарушителей информационной безопасности автоматизированных систем	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владениенеприобретено				
ПСК-7.2	Знать теоретические основы риск-анализа информационной безопасности автоматизированных систем	2 - полное освоение знания 1 – неполное освоение знания 0 – знаниенеосвоено				
	Уметь применять на практике	2 - полное				

	методы оценки ущербов и вероятности их наступления в условиях нарушения информационной безопасности автоматизированных систем	приобретение умения 1 – неполное приобретение умения 0 – умениенеприобретено				
	Владеть навыками комплексной оценки рисков и защищенности автоматизированных систем	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владениенеприобретено				
ПСК-7.3	Знать принципы организации аудита защищенности ресурсов распределенных информационных систем	2 - полное освоение знания 1 – неполное освоение знания 0 – знаниенеосвоено				
	Уметь применять на практике приемы и средства аудита защищенности информационно-технологических ресурсов распределенных информационных систем	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умениенеприобретено				
	Владеть навыками проведения комплексного аудита и выработки предложений по усовершенствованию политики защиты информационно-технологических ресурсов распределенных информационных систем	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владениенеприобретено				
ПСК-7.4	Знать принципы организации удаленного администрирования операционных систем и систем баз данных в распределенных информационных системах	2 - полное освоение знания 1 – неполное освоение знания 0 – знаниенеосвоено				
	Уметь организовывать на практике удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умениенепри				

		обретено				
	Владеть навыками комплексного администрирования операционных систем и баз данных распределенных информационных систем	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владениенеприобретено				
ПСК-7.5	Знать теоретические основы организационного управления в области обеспечения информационной безопасности автоматизированных систем	2 - полное освоение знания 1 – неполное освоение знания 0 – знаниенеосвоено				
	Уметь координировать деятельность подразделений и специалистов в отдельно взятой организации	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умениенеприобретено				
	Владеть навыками комплексной оценки эффективности деятельности подразделений и специалистов по защите информации в организациях	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владениенеприобретено				

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. (474Кб). - Воронеж : ФГБОУ ВПО "Воронежскийгосударственныйтехническийуниверситет", 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 "Воронежскийгосударственныйтехническийуниверситет", 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,НЕОБХОДИМАЯДЛЯПРОВ

ЕДЕНИЯПРАКТИКИ

Специализированнаялекционнаяаудитория, оснащенная оборудованием для лекционных демонстраций и проекционной аппаратурой.