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 10.05.01 КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

Специализация «Безопасность распределенных компьютерных систем»

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2017

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–ПроизводственнаяпрактикаТиппрактика–Преддипломнаяпрактика Формапроведенияпрактики–дискретно

Способпроведенияпрактики–стационарная,выездная.

Стационарнаяпрактикапроводитсявпрофильныхорганизациях,расположеннойнатерриторииг.Воронежа.

Выезднаяпрактикапроводитсявместахпроведенияпрактик,расположенныхвнег.Воронежа.

Способпроведенияпрактикиопределяетсяиндивидуальнодлякаждогостудентаиуказываетсявприказенапрактику.

Местопроведенияпрактики–переченьобъектовдляпрохожденияпрактикиустанавливаетсянаосноветиповыхдвусторонниххдоговоровмеждупредприятиями(организациями)иВУЗомилиВУЗ.

3.МЕСТОПРАКТИКИВСТРУКТУРЕОПОП

Практика«Преддипломнаяпрактика»относитсякбазовойчастиблока Б2.

4.ПЕРЕЧЕНЬПЛАНИРУЕМЫХРЕЗУЛЬТАТОВОБУЧЕНИЯПРИПРОХОЖДЕНИИПРАКТИКИ,СООТНЕСЕННЫХСПЛАНИРУЕМЫМИРЕЗУЛЬТАТАМИОСВОЕНИЯОБРАЗОВАТЕЛЬНОЙПРОГРАММЫ

Процесспрохожденияпрактики«Преддипломнаяпрактика»направленна формированиеследующихкомпетенций:

ОПК-1-способностьюанализироватьфизическиеявленияипроцессыприрешениипрофессиональныхзадач

ОПК-2-способностьюкорректноприменятьприрешениипрофессиональныхзадачаппаратматематическогоанализа,геометрии,алгебры,дискретноймате матики,математическойлогики,теорииалгоритмов,теориивероятностей,математическойстатистики,теорииинформации,теоретико-числовыхметодов

ОПК-5-способностьюиспользоватьнормативныеправовыеактывсвоейпрофессиональнойдеятельности

ОПК-7-способностьюучитыватьсовременныетенденцииразвитияинформатикиивычислительнойтехники,компьютерныхтехнологийвсвоейпрофессиональнойдеятельности,работатьспрограммнымисредствамиобщегоиспециальногоназначения

ОПК-9-способностьюразрабатыватьформальныемоделиполитикбезопасности,политикуправлениядоступомиинформационнымипотокамивкомпьютерныхсистемахсучетомугрозбезопасностиинформации

ПК-3-способностьюпроводитьанализбезопасностикомпьютерныхсистемнасоответствиеотечественнымизарубежнымстандартамвобластикомпьютернойбезопасности

ПК-4-способностьюпроводитьанализиучаствоватьвразработкематематическихмоделейбезопасностикомпьютерныхсистем

ПК-5-способностьюучаствоватьвразработкеиконфигурированиипрограммно-аппаратныхсредствзащитыинформации,включаязащищенныеоперационныесистемы,системыуправлениябазамиданных,компьютерныесети,системыантивирусной защиты,средствакриптографическойзащитыинформации

ПК-7-способностьюпроводитьанализпроектныхрешенийпообеспечениюзащищенностикомпьютерныхсистем

ПК-14-способностьюорганизовыватьработыповыполнениюрежимазащитыинформации,втомчислеограниченногодоступа

ПСК-3.1-способностьюиспользоватьсовременныекритериииистандартыдляанализабезопасностираспределенныхкомпьютерныхсистем

ПСК-3.2-способностьюанализироватьзащитуинформациивраспределенныхкомпьютерныхсистемах,проводитьмониторинг,аудитиконтрольныепроверкиработоспособностиизащищенностираспределенныхкомпьютерныхсистем

ПСК-3.3-способностьюиспользоватьсовременныесредыитехнологии,разработкипрограммногообеспечениявраспределенныхкомпьютерныхсистемахсучетомтребованийинформационнойбезопасности

ПСК-3.4-способностьюорганизовыватьзащитуинформациивраспределенныхкомпьютерныхсистемах

ПСК-3.5-способностьюучаствоватьвформировании,реализацииконтролеэффективностиполитикиинформационнойбезопасностираспределенныхкомпьютерныхсистем

Компетенция	**Результатыобучения,характеризующие сформированностькомпетенции**
ОПК-1	Знать теоретические основы и задачи физики и математики в контексте обеспечения компьютерной безопасности
	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 компьютерной безопасности
ОПК-2	Знать теоретические основы алгебры, геометрии, математического анализа, теории вероятности, математической статистики, математической логики, теории алгоритмов, теории информации в контексте обеспечения компьютерной безопасности
	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 компьютерной безопасности
	Владеть методами математического исследования процессов нарушения компьютерной безопасности
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
ОПК-7	Знать методы техники безопасностипри работе спрборами иоборудованием длязащиты информации
	Уметь применять на практике работу с офиснойтехникой испециализированнымоборудованием с учетомтребований техникибезопасности
	Владетьнавыками работыс измерительнымиприборами итиповымоборудованиемдля защитыинформации
ОПК-9	Знать методы разработкиформальныхмоделейполитикбезопасности, политикуправлениядоступомиинформационнымипотокамивкомпьютерныхсистемахсучетомугрозбезопасности информации
	Уметь применять на практике работу с моделями политик безопасности, управления доступом и информационными потоками
	Владеть навыками работы с моделями политик безопасности, управления доступом и информационными потоками
ПК-3	Знатьтеоретические и практические основы средств обеспечения компьютерной безопасности данных

	Уметьприменять на практике основныезаконы и нормативныедокументы в области компьютерной безопасности
	Владетьнавыками анализаосновных узловустройствсовременных компьютерных систем
ПК-4	Знать теоретические основы моделирования угроз и нарушителей компьютерной безопасности
	Уметь разрабатывать модели угроз и нарушителей компьютерной безопасности
	Владеть приемами практического применения моделей угроз и нарушителей компьютерной безопасности
ПК-5	Знать теоретические основы конфигурирования программно-аппаратныхсредствзащитыинформации
	Уметь применять на практике политику обеспечения компьютерной безопасности
	Владеть навыкамизащитыинформации,включаязащищенныеоперационныесистемы,системыуправлениябазамиданных,компьютерныесети,системыантивирусной защиты,средствакриптографическойзащитыинформации
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-14	Знать теоретические и практические основыорганизацииработыповыполнениюрежимазащитыинформации,втомчислеограниченногодоступа
	Уметьучаствовать в контрольных проверкахработоспособности применяемых программно-аппаратных средств для обеспечения компьютерной безопасности
	Владеть навыками, приемами защиты информации и основами организацииработыповыполнениюрежимазащитыинформации
ПСК-3.1	Знатьтеоретические основы анализабезопасностираспределенныхкомпьютерныхсистем
	Уметь применять на практике профессиональные навыки в сфере анализабезопасностираспределенныхкомпьютерныхси

	стем
	Владеть современнымикритериямиистандартамидляанализабезопасностираспределенныхкомпьютерныхсистем
ПСК-3.2	Знать теоретические основы в сфере защиты информации распределенных компьютерных систем
	Уметьприменять на практике анализзащитыинформациивраспределенныхкомпьютерныхсистемах
	Владеть навыками мониторинга,аудитаиконтрольныхпроверокработоспособностиизащищенностираспределенныхкомпьютерныхсистем
ПСК-3.3	Знать теоретические основы в сфере защиты информации распределенных компьютерных систем
	Уметь применять на практике защитуинформациивраспределенныхкомпьютерныхсистемах
	Владеть навыками обеспечения защиты информации враспределенныхкомпьютерныхсистемах
ПСК-3.4	Знать организационные навыки защитыинформациивраспределенныхкомпьютерныхсистемах
	Уметьорганизовыватьзащитуинформациивраспределенныхкомпьютерныхсистемах
	Владеть навыками обеспечения профессиональной организации защитыинформациивраспределенныхкомпьютерныхсистемах
ПСК-3.5	Знать теоретические основы политикиинформационнойбезопасностираспределенныхкомпьютерныхсистем
	Уметь применять на практике формирование, реализацию и контроль эффективности политикиинформационнойбезопасностираспределенныхкомпьютерныхсистем
	Владетьспособностьюучаствоватьвформировании,реализацииконтролеэффективностиполитикиинформационнойбезопасностираспределенныхкомпьютерныхсистем

5. ОБЪЕМ ПРАКТИКИ

Общийобъемпрактикисоставляетсоставляет21з.е.,еепродолжительность – 14недель.

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.	*732*
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	*756*

7.ОЦЕНОЧНЫЕМАТЕРИАЛЫДЛЯПРОВЕДЕНИЯПРОМЕЖУТОЧНОЙАТТЕСТАЦИИПОПРОХОЖДЕНИЮПРАКТИКИ

7.1Подготовкаотчетаопрохожденииипрактики

Аттестацияпоитогампрактикипроводитсяввидезачетасоценкойнаосновеэкспертнойоценкидеятельностиобучающегосяизащитыотчета.Позавершениипрактикистудентывпоследнийденьпрактикипредставляютнавыпускающуюкафедру:дневникпрактики,включающийвсебяотзывыруководителейпрактикиотпредприятияиВУЗаоработестудентавпериодпрактикисоценкойуровняиоперативностивыполненияимзаданияпопрактике,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

Результатыпромежуточногоконтролязнанийоцениваютсяв11семестредляочнойформыобученияпочетырехбалльнойсистеме:

«отлично»;
«хорошо»;

«удовлетворительно»;
«неудовлетворительно».

Компе-тенция	Результатыобучения,характеризующие сформированностькомпетенции	Экспертнаяоценкарезультатов	Отлично	Хорошо	Удовл.	Неудовл.
ОПК-1	Знать теоретические основы и задачи физики и математики в контексте обеспечения компьютерной безопасности	2 - полное освоение знания 1 – неполное освоение знания 0 – знание не освоено	Более 80% от максимально возможного количества баллов	61%-80% от максимально возможного количества баллов	41%-60% от максимально возможного количества баллов	Менее 41% от максимально 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 – умение не приобретено				
	Владеть моделями и методиками физико-математического моделирования процессов нарушения компьютерной безопасности	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владение не приобретено				
ОПК-2	Знать теоретические основы алгебры, геометрии, математического анализа, теории вероятности, математической статистики, математической логики, теории алгоритмов, теории информации в контексте обеспечения компьютерной безопасности	2 - полное освоение знания 1 – неполное освоение знания 0 – знание не освоено				
	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 компьютерной безопасности	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умение не приобретено				
	Владеть методами математического исследования процессов	2 - полное приобретение владения 1 – неполное приобретение				

	нарушения компьютерной безопасности	владения 0 – владение не приобретено				
ОПК -5	Знать методы научных исследований в профессиональной деятельности	2 - полное освоение знания 1 – неполное освоение знания 0 – знание не освоено				
	Уметь применять теоретическую базу для проектирования программного обеспечения и устройств	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умение не приобретено				
	Владеть навыками и методами создания программного обеспечения и устройств для решения профессиональных задач	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владение не приобретено				
ОПК -7	Знать методы техники безопасности при работе с приборами и оборудованием для защиты информации	2 - полное освоение знания 1 – неполное освоение знания 0 – знание не освоено				
	Уметь применять на практике работу с офисной техникой и специализированным оборудованием с учетом требований техники безопасности	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умение не приобретено				
	Владеть навыками работы с измерительными приборами и типовым оборудованием для защиты информации	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владение не приобретено				
ОПК -9	Знать методы разработки формальных моделей политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации	2 - полное освоение знания 1 – неполное освоение знания 0 – знание не освоено				
	Уметь применять на практике работу с моделями политик безопасности, управления доступом и информационными потоками	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умение не приобретено				
	Владеть навыками работы с моделями политик безопасности, управления доступом и информационными потоками	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владение не приобретено				
ПК-3	Знать теоретические и практические основы	2 - полное освоение знания 1 – неполное освоение				

	средств обеспечения компьютерной безопасности данных	знания 0 – знание не освоено				
	Уметь применять на практике основные законы и нормативные документы в области компьютерной безопасности	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умение не приобретено				
	Владеть навыками анализа основных узлов устройств современных компьютерных систем	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владение не приобретено				
ПК-4	Знать теоретические основы моделирования угроз и нарушителей компьютерной безопасности	2 - полное освоение знания 1 – неполное освоение знания 0 – знание не освоено				
	Уметь разрабатывать модели угроз и нарушителей компьютерной безопасности	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умение не приобретено				
	Владеть приемами практического применения моделей угроз и нарушителей компьютерной безопасности	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владение не приобретено				
ПК-5	Знать теоретические основы конфигурирования программно-аппаратных средств защиты информации	2 - полное освоение знания 1 – неполное освоение знания 0 – знание не освоено				
	Уметь применять на практике политику обеспечения компьютерной безопасности	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умение не приобретено				
	Владеть навыками защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владение не приобретено				
ПК-7	Знать основы работы с научно-технической документацией	2 - полное освоение знания 1 – неполное освоение знания 0 – знание не освоено				
	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 – владение не приобретено				
ПК-14	Знать теоретические и практические основы организации работы по выполнению режима защиты информации, в том числе ограниченного доступа	2 - полное освоение знания 1 – неполное освоение знания 0 – знание не освоено				
	Уметь участвовать в контрольных проверках работоспособности применяемых программно-аппаратных средств для обеспечения компьютерной безопасности	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умение не приобретено				
	Владеть навыками, приемами защиты информации и основами организации работы по выполнению режима защиты информации	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владение не приобретено				
ПСК-3.1	Знать теоретические основы анализа безопасности распределенных компьютерных систем	2 - полное освоение знания 1 – неполное освоение знания 0 – знание не освоено				
	Уметь применять на практике профессиональные навыки в сфере анализа безопасности распределенных компьютерных систем	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умение не приобретено				
	Владеть современными критериями и стандартами для анализа безопасности распределенных компьютерных систем	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владение не приобретено				
ПСК-3.2	Знать теоретические основы в сфере защиты информации распределенных компьютерных систем	2 - полное освоение знания 1 – неполное освоение знания 0 – знание не освоено				
	Уметь применять на практике анализ защиты информации в распределенных компьютерных системах	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умение не приобретено				
	Владеть навыками мониторинга, аудита и контрольных проверок работоспособности и защищенности распределенных компьютерных систем	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владение не приобретено				

ПСК -3.3	Знать теоретические основы в сфере защиты информации распределенных компьютерных систем	2 - полное освоение знания 1 – неполное освоение знания 0 – знание не освоено				
	Уметь применять на практике защиту информации в распределенных компьютерных системах	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умение не приобретено				
	Владеть навыками обеспечения защиты информации в распределенных компьютерных системах	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владение не приобретено				
ПСК -3.4	Знать организационные навыки защиты информации в распределенных компьютерных системах	2 - полное освоение знания 1 – неполное освоение знания 0 – знание не освоено				
	Уметь организовывать защиту информации в распределенных компьютерных системах	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умение не приобретено				
	Владеть навыками обеспечения профессиональной организации защиты информации в распределенных компьютерных системах	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владение не приобретено				
ПСК -3.5	Знать теоретические основы политики информационной безопасности распределенных компьютерных систем	2 - полное освоение знания 1 – неполное освоение знания 0 – знание не освоено				
	Уметь применять на практике формирование, реализацию и контроль эффективности политики информационной безопасности распределенных компьютерных систем	2 - полное приобретение умения 1 – неполное приобретение умения 0 – умение не приобретено				
	Владеть способностью участвовать в формировании, реализации и контроле эффективности политики информационной безопасности распределенных компьютерных систем	2 - полное приобретение владения 1 – неполное приобретение владения 0 – владение не приобретено				

Экспертнаяоценкарезультатовосвоениякомпетенцийпроизводитсяруководителемпрактики(илисогласованнаяоценкаруководителяпрактикиотВУЗаируководителяпрактикиотоорганизации).

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,включаяпереченьлицензи

онногопрограммногообеспечения,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

Специализированнаялекционнаяаудитория, оснащенная оборудованием для лекционных демонстраций и проекционной аппаратурой.