Министерство науки и высшего образования Российской Федерации

Калужский филиал федерального государственного бюджетного образовательного учреждения высшего образования
«Московский государственный технический университет имени Н.Э. Баумана
(национальный исследовательский университет)»
(КФ МГТУ им. Н.Э. Баумана)

Утверждаю
Зам. директора
КФ МГТУ им. Н.Э. Баумана
по учебной работе
_____ О.Л. Перерва
«11» 01 2019 г.

Регистрационный номер ПД.ИУ6-20/19

Факультет «Информатика и управление» (ИУ-КФ)

Кафедра «Защита информации» ИУ6-КФ

ПРОГРАММА ПРАКТИКИ

Производственная практика

Вид практики

Преддипломная практика

Тип практики

для специальности 10.05.03 «Информационная безопасность автоматизированных систем»

специалиста (специализация «Анализ безопасности информационных систем»)

Автор(ы) программы:

Твердова С.М., к.т.н., доцент, TverdovaSM@bmstu-kaluga.ru

Калуга, 2019

Автор(ы) программы:

Твердова С.М. _____

Рецензент:
Директор
АО «Калуга Астрал»

Чернин И.И. _____

Утверждена на заседании кафедры ИУ6-КФ «Защита информации»
Протокол №06 от «10» 01 2019г.
Заведующий кафедрой ИУ6-КФ «Защита информации»

Мазин А.В. _____

Декан факультета ИУ-КФ

Алкин М.Ю. _____

Согласовано:

Председатель Методической комиссии КФ МГТУ им. Н.Э. Баумана

Перерва О.Л. _____

ОГЛАВЛЕНИЕ

Программа разработана в соответствии с учебным планом КФ МГТУ им. Н.Э. Баумана по специальности 10.05.03 Информационная безопасность автоматизированных систем (специализация– «Анализ безопасности информационных систем»).

1. ВИД ПРАКТИКИ, СПОСОБ И ФОРМЫ ЕЕ ПРОВЕДЕНИЯ

1.1 Вид практики – производственная, тип практики – преддипломная.

1.2. Способы проведения практики – стационарная.

1.3. Практика проводится дискретно по видам практик – путем выделения в календарном учебном графике непрерывного периода учебного времени для проведения каждого вида (совокупности видов) практики.

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

Для категорий «знания», «умения» и «навыки» планируется достижение следующих результатов обучения при прохождении практики, соотнесенных с планируемыми результатами освоения образовательной программы – формируемыми компетенциями:

- способность использовать языки, системы, инструментальные программные и аппаратные средства для моделирования информационных систем и испытаний систем защиты (ПСК-1.1);

Результаты обучения при прохождении практики, соотнесенные с компетенцией		
Обучающийся должен знать:	Обучающийся должен уметь:	Обучающийся должен владеть:
- понятия моделирования, испытания; - методы моделирования систем защиты; - подходы проведения испытаний систем защиты	- программировать на языках высокого и низкого уровней, - работать с инструментальными средствами моделирования	- навыками использования языков, систем, инструментальных программных и аппаратных средств для моделирования информационных систем и испытаний систем защиты

- способность разрабатывать методики и тесты для анализа степени защищенности информационной системы, соответствия нормативным требованиям по защите информации (ПСК-1.2);

Результаты обучения при прохождении практики, соотнесенные с компетенцией		
Обучающийся должен знать:	Обучающийся должен уметь:	Обучающийся должен владеть:
- документы, регламентирующие нормативные требования по защите информации; - понятия методики, теста; - порядок проведения тестов для анализа степени защищенности информационной системы;	- составлять план проведения тестирования для анализа степени защищенности информационной системы	- навыками разработки методик и тестов для анализа степени защищенности информационной системы, соответствия нормативным требованиям по защите информации

- существующие методики анализа степени защищенности		

- способность осуществлять математическую постановку задачи и решать ее современными оптимизационными методами для оптимального выбора средств защиты информации при ограничениях на их стоимость, габариты, энергопотребление и др. (СПК-9);

Результаты обучения при прохождении практики, соотнесенные с компетенцией		
Обучающийся должен знать:	Обучающийся должен уметь:	Обучающийся должен владеть:
- современные методы оптимизации; - классы наиболее распространенных задач принятия решений; - критерии оценки качества оптимизации.	- разрабатывать математическую модель оптимизационной задачи; - назначать параметры оптимизации; - формировать критерии качества, позволяющие оценить полученное решение.	- навыками осуществления математической постановки задачи и решения ее современными оптимизационными методами для оптимального выбора средств защиты информации при ограничениях на их стоимость, габариты, энергопотребление и др.

- способность разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем (СПК-12);

Результаты обучения при прохождении практики, соотнесенные с компетенцией		
Обучающийся должен знать:	Обучающийся должен уметь:	Обучающийся должен владеть:
- понятие безопасности автоматизированных систем; - нормативные документы по обеспечению безопасности автоматизированных систем.	- выявлять угрозы и уязвимости информационной безопасности в автоматизированной системе.	- навыками разработки и анализа проектных решений по обеспечению безопасности автоматизированных систем.

- способность участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности (СПК-13);

Результаты обучения при прохождении практики, соотнесенные с компетенцией		
Обучающийся должен знать:	Обучающийся должен уметь:	Обучающийся должен владеть:
- нормативно – правовые документы, регламентирующие разработку автоматизированных систем в защищенном исполнении.	- разрабатывать проекты защищенных автоматизированных систем; - оформлять проектную документацию.	- навыками участия в разработке защищенных автоматизированных систем в сфере профессиональной деятельности.

- способность применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности (СПК-14);

Результаты обучения при прохождении практики, соотнесенные с компетенцией		
Обучающийся должен знать:	Обучающийся должен уметь:	Обучающийся должен владеть:
- современную электронную компонентную базу, принципы работы электронных компонентов и физические процессы, протекающие в них;	- пользоваться нормативными документами; - применять компонентную базу; - применять технологи, методы и языки программиро-	- навыками применения знаний в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разра-

- современные методы, технологии и языки программирования.	вания.	ботке программно- аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности.

- способность участвовать в проектировании средств защиты информации автоматизированной системы (СПК-17);

Результаты обучения при прохождении практики, соотнесенные с компетенцией		
Обучающийся должен знать:	Обучающийся должен уметь:	Обучающийся должен владеть:
- нормативно – правовую базу в области защиты информации; - принципы проектирования программного и аппаратного обеспечения.	- программировать на языках высокого и низкого уровней; - применять современную электронную компонентную базу; - оформлять проектную и конструкторскую документацию.	- навыками участия в проектировании средств защиты информации автоматизированной системы.

- способность разрабатывать конструкторскую, технологическую и ремонтную документацию на программные, технические и программно-аппаратные средства защиты (СПК-21);

Результаты обучения при прохождении практики, соотнесенные с компетенцией		
Обучающийся должен знать:	Обучающийся должен уметь:	Обучающийся должен владеть:
- виды документации на программные, технические и программно-аппаратные средства защиты.	- создавать и редактировать тексты профессионального назначения; - оформлять документы по требованиям с помощью текстового редактора; - использовать редактор формул; - использовать графический пакет для оформления схем.	- навыками разработки конструкторской, технологической и ремонтной документации на программные, технические и программно-аппаратные средства защиты.

- способность осуществлять разработку аппаратно – программных средств обеспечения информационной безопасности, применимых как в Российской Федерации, так и в других странах мира, и ориентированных на международно признанные стандарты в области защиты информации (СПК-22);

Результаты обучения при прохождении практики, соотнесенные с компетенцией		
Обучающийся должен знать:	Обучающийся должен уметь:	Обучающийся должен владеть:
- российские и международные стандарты в области защиты информации; - технологии разработки программных и аппаратных средств; - структуру и принципы работы современных и перспективных микропроцессоров	- проводить проектирование аппаратных и программных средств, - программировать на языках высокого и низкого уровня; - выбирать элементную базу; - разрабатывать схемы аппаратных или аппаратно- программных средств, моделировать разработанные схемы	- навыками осуществления разработки аппаратно – программных средств обеспечения информационной безопасности

- способность проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации (СПК-23);

Результаты обучения при прохождении практики, соотнесенные с компетенцией		
Обучающийся должен знать:	Обучающийся должен уметь:	Обучающийся должен владеть:
- понятие контрольной проверки работоспособности; - порядок проведения контрольной проверки работоспособности программно-аппаратных, криптографических и технических средств; - критерии работоспособности программно-аппаратных, криптографических и технических средств; - рекомендации по составлению плана проведения контрольных проверок программно-аппаратных, криптографических и технических средств	- разрабатывать план проведения контрольных проверок работоспособности применяемых программно- аппаратных, криптографических и технических средств; - оценивать результаты проведенных проверок работоспособности; - оформлять отчет о проведенных проверках работоспособности	- навыками проведения контрольных проверок работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации.

- способность участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем (СПК-24);

Результаты обучения при прохождении практики, соотнесенные с компетенцией		
Обучающийся должен знать:	Обучающийся должен уметь:	Обучающийся должен владеть:
- понятие сертификации средств защиты информации; - порядок проведения сертификационных испытаний. - виды оформляемых документов на сертификацию.	- оформлять документов по результатам проведения экспериментально-исследовательских работ при сертификации средств защиты информации в соответствии с установленными требованиями.	- навыками участия в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем

- способность проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации (СПК-26);

Результаты обучения при прохождении практики, соотнесенные с компетенцией		
Обучающийся должен знать:	Обучающийся должен уметь:	Обучающийся должен владеть:
- понятия мониторинга защищенности информации в автоматизированной системе, канала утечки информации; - средства инструментального мониторинга защищенности информации в автоматизированной системе и выявления каналов утечки ин-	- применять средства инструментального мониторинга.	- навыками проведения инструментального мониторинга защищенности информации в автоматизированной системе и выявлять каналы утечки информации.

формации.		

- способность планировать и проводить анализ защищенности автоматизированных систем путем тестирования на проникновение (СПК-27);

Результаты обучения при прохождении практики, соотнесенные с компетенцией		
Обучающийся должен знать:	Обучающийся должен уметь:	Обучающийся должен владеть:
- понятие анализа защищенности; - подходы анализа защищенности автоматизированных систем; - средства тестирования на проникновение.	- применять средства тестирования на проникновение.	- навыками планирования и проведения анализа защищенности автоматизированных систем путем тестирования на проникновение

- способность организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности (СПК-28);

Результаты обучения при прохождении практики, соотнесенные с компетенцией		
Обучающийся должен знать:	Обучающийся должен уметь:	Обучающийся должен владеть:
- принципы организации работ малых коллективов исполнителей; - подходы выработки и реализации управленческих решений.	- разрабатывать и оформлять распорядительную документацию.	- навыками организации работы малых коллективов исполнителей, выработки и реализации управленческих решений в сфере профессиональной деятельности.

Виды профессиональной деятельности, к которым готовится обучающийся при прохождении практики:

– научно-исследовательская деятельность;

– проектно-конструкторская деятельность;

– контрольно-аналитическая деятельность;

– организационно-управленческая деятельность.

Обучающийся при прохождении практики в соответствии с видами профессиональной деятельности готовится решать следующие **профессиональные задачи**:

– анализ защищенности информации в автоматизированных системах и безопасности реализуемых информационных технологий;
– разработка эффективных решений по обеспечению информационной безопасности автоматизированных систем;
– разработка защищенных автоматизированных систем в сфере профессиональной деятельности, обоснование выбора способов и средств защиты информационно-технологических ресурсов автоматизированных систем;
– выполнение проектов по созданию программ, комплексов программ, программно-аппаратных средств, баз данных, компьютерных сетей для защищенных автоматизированных систем;
– выполнение экспериментально-исследовательских работ при сертификации средств защиты информации и аттестации автоматизированных систем;
– проведение инструментального мониторинга защищенности автоматизированных систем и анализа его результатов;

– организация работы коллектива, принятие управленческих решений в условиях спектра мнений, определение порядка выполнения работ;
– использование языков, систем, инструментальных программных и аппаратных средства для моделирования информационных систем и испытаний систем защиты, в том числе анализа безопасности программного обеспечения.
Объектами профессиональной деятельности выпускников, успешно прошедших практику в составе образовательной программы, являются:

– автоматизированные системы, функционирующие в условиях существования угроз в информационной сфере и обладающие информационно-технологическими ресурсами, подлежащими защите;

– технологии обеспечения информационной безопасности автоматизированных систем.

3. МЕСТО ПРАКТИКИ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Учебная практика входит в Блок 2 «Практики, в том числе научно-исследовательская работа (НИР)».
Прохождение практики предполагает предварительное освоение следующих дисциплин (практик) учебного плана: Языки программирования, Электроника и схемотехника, Аппаратные средства вычислительной техники, Теоретические основы информационной безопасности автоматизированных систем, Криптографические методы защиты информации, Технические средства защиты информации, Государственная система защиты информации, Программно – аппаратные средства обеспечения информационной безопасности, Основы управленческой деятельности, Учебно – технологический практикум, Ознакомительная практика, Учебная практика, Технологическая практика, Профессиональная практика.
Результаты прохождения практики необходимы как предшествующие для выполнения и защиты выпускной квалификационной работы.

4. ОБЪЕМ ПРАКТИКИ И ЕЕ ПРОДОЛЖИТЕЛЬНОСТЬ

	Всего	Продолжительность и объем по семестрам
		12 семестр 4 недели
Объем практики, з.е.	**6**	**6**
Объем практики, час.	216	216
Промежуточная аттестация		Зачет

5. СОДЕРЖАНИЕ ПРАКТИКИ

№ пп	Этапы практики	Час.
	12 семестр	216
5.1	Разработка проектных решений по организации защищенных автоматизированных систем	64
5.2	Разработка программно – аппаратных средств защиты информации	64
5.3	Проведение контрольно – аналитической работы в сфере защиты информации	56
5.4	Организационная работа в сфере обеспечения информационной безопасности	16
5.5	Оформление отчета о проведенной работе	15

5.6	Промежуточная аттестация	1

Содержание

5.1 Разработка проектных решений по организации защищенных автоматизированных систем

Цель: сформировать первичные профессиональные умения и навыки осуществления математической постановки задачи и решения ее современными оптимизационными методами для оптимального выбора средств защиты информации при ограничениях на их стоимость, габариты, энергопотребление и др.; разработки и анализа проектных решений по обеспечению безопасности автоматизированных систем; участия в разработке защищенных автоматизированных систем в сфере профессиональной деятельности.

Задачи: провести анализ существующих решений по обеспечению безопасности автоматизированной системы предприятия или его структурного подразделения, при необходимости разработать проектное решение, совершенствующее существующее; сформулировать задачу выбора средств защиты информации при ограничениях на их определенные параметры для рассматриваемой АС, записать математическую постановку задачи и решить ее; принять участие в разработке защищенной автоматизированной системы предприятия – базы практики.

5.2 Разработка программно – аппаратных средств защиты информации

Цель: сформировать первичные профессиональные умения и навыки применения знаний в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно- аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности; участия в проектировании средств защиты информации автоматизированной системы; разработки конструкторской, технологической и ремонтной документации на программные, технические и программно-аппаратные средства защиты; осуществления разработки аппаратно – программных средств обеспечения информационной безопасности.

Задачи: провести проектирование средства защиты информации (программного, аппаратного, программно – аппаратного или технического) с учетом российских и международно признанных стандартов в области защиты информации; разработать конструкторскую, технологическую и ремонтную документацию на разрабатываемое средство защиты информации.

5.3 Проведение контрольно – аналитической работы в сфере защиты информации

Цель: проведения контрольных проверок работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации; участия в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем; проведения инструментального мониторинга защищенности информации в автоматизированной системе и выявлять каналы утечки информации; планирования и проведения анализа защищенности автоматизированных систем путем тестирования на проникновение.

Задачи: разработать методики и тесты для проверки работоспособности разработанного средства защиты информации; для анализа степени защищенности информационной системы, соответствия нормативным требованиям по защите информации; для проведения экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем; провести инструментальный мониторинг защищенности информации в рассматриваемой автоматизированной системе, по возможности выявлять каналы утечки информации.

5.4 Организационная работа в сфере обеспечения информационной безопасности

Цель: сформировать первичные профессиональные умения и навыки организации работы малых коллективов исполнителей, выработки и реализации управленческих решений в сфере профессиональной деятельности.

Задача: разработать и оформить распорядительную и эксплуатационную документацию по организации работы с разрабатываемым средством защиты информации.

5.5 Оформление отчета о проведенной работе

Цель: сформировать первичные профессиональные умения и навыки осуществления разработки аппаратно – программных средств обеспечения информационной безопасности и проведения контрольных проверок работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации.

Задача: оформить отчет о проделанной работе в соответствии с требованиями с использованием современных информационных технологий.

5.6 Промежуточная аттестация

Промежуточная аттестация проводится с учетом своевременности выполнения заданий, качества выполнения заданий и защиты полученных результатов.

6. ФОРМА ОТЧЕТНОСТИ ПО ПРАКТИКЕ

Преддипломная практика проводится для выполнения выпускной квалификационной работы. Выполнение выпускной квалификационной работы в период преддипломной практики представляет собой деятельность студента, направленную на подготовку, обобщение, структурирование и оформление расчетных, графических, презентационных и иных материалов по результатам самостоятельно выполненных студентом в период обучения научно-исследовательских, педагогических и производственно-технологических профессионально-ориентированные работ.

Форма отчетности по практике – подготовленный материал для расчетно – пояснительной записки выпускной квалификационной работы. Структура и содержание ВКР определяется Программой государственной итоговой аттестации.

Выпускная квалификационная работа выполняется обучающимся самостоятельно в соответствии с утвержденным календарным графиком.

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ПРАКТИКЕ

Фонд оценочных средств приведен в приложении к программе практики и включает в себя:

– перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы;

– типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы;

– описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания;

– методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

8. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ И РЕСУРСОВ СЕТИ "ИНТЕРНЕТ", НЕОБХОДИМЫХ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ

Основная литература

1.Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации [Электронный ресурс]: учебное пособие / Ю. Н. Загинайлов. – М.-Берлин: Изд-во «Директ-Медиа», 2015. – 253 с. – URL: http://biblioclub.ru/index.php?page=book&id=276557
2. Васильков, А.В. Информационные системы и их безопасность [Текст] : учеб. пособие / А.В. Васильков, А.А. Васильков, И.А. Васильков. – М.: Изд-во «Форум», 2013. – 528 с.
3.Торгонский, Л.А. Проектирование центральных и периферийных устройств ЭВС [Электронный ресурс] : учебное пособие / Л.А. Торгонский, П.Н. Коваленко ; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). - Томск: Эль Контент, 2012. - Ч. II. Микропроцессорные ЭВС. - 176 с. URL: http://biblioclub.ru/index.php?page=book&id=208701
4. Галас, В. П. Вычислительные системы, сети и телекоммуникации. Часть 1. Вычислительные системы [Электронный ресурс] : электронный учебник / В. П. Галас. — Владимир : Владимирский государственный университет им. А.Г. и Н.Г. Столетовых, 2016. — 232 с. — URL: http://www.iprbookshop.ru/57363.html
5. Галас, В. П. Вычислительные системы, сети и телекоммуникации. Часть 2. Сети и телекоммуникации[Электронный ресурс] : электронный учебник / В. П. Галас. — Владимир : Владимирский государственный университет им. А.Г. и Н.Г. Столетовых, 2016. — 311 с. — URL: http://www.iprbookshop.ru/57364.html
6. Царев, Р.Ю. Программирование на языке Си [Электронный ресурс]: учебное пособие / Р.Ю. Царев. – Красноярск: Сибирский федеральный университет, 2014. – 108 с. – URL: http://biblioclub.ru/index.php?page=book&id=364601

Дополнительная литература

7. Лехин С.Н. Схемотехника ЭВМ [Текст] : учеб. пособие/С.Н.Лехин.-СПб.:БХВ-Петербург,2010.-672с.

8. Виноградов, В. И. Элементы и узлы ЭВМ. Часть 1 [Электронный ресурс] : методические указания к лабораторному практикуму по курсу «Элементы и узлы ЭВМ» / В. И. Виноградов, С. Б. Спиридонов, А. В. Шигин. — М. : Московский государственный технический университет имени Н.Э. Баумана, 2009. — 12 с. —URL: http://www.iprbookshop.ru/31329.html

9. Виноградов, В. И. Элементы и узлы ЭВМ. Часть 2 [Электронный ресурс]: методические указания к лабораторному практикуму по курсу «Элементы и узлы ЭВМ» / В. И. Виноградов, С. Б. Спиридонов, А. В. Шигин. — М. : Московский государственный технический университет имени Н.Э. Баумана, 2011. — 20 с— URL: http://www.iprbookshop.ru/31363.html

Ресурсы сети «Интернет»

1. Российская государственная библиотека. http://www.rsl.ru.
2. Российская национальная библиотека. http://www.nlr.ru.
3. Государственная публичная научно-техническая библиотека России. http://www.gpntb.ru.
4. Библиотека МГТУ им. Н.Э. Баумана. http://library.bmstu.ru.
5. Научно-техническая библиотека КФ МГТУ им. Н.Э. Баумана. http://library.bmstu-kaluga.ru.
6. Центральная библиотека образовательных ресурсов Минобрнауки РФ. www.edulib.ru.
7. Российская библиотека интеллектуальной собственности. http://www.rbis.su/index.php.

9. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ПРОВЕДЕНИИ ПРАКТИКИ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ (ПРИ НЕОБХОДИМОСТИ)

Информационные технологии

Предусмотрена возможность асинхронного взаимодействия студентов и преподавателей посредством технологий и служб по пересылке и получению электронных сообщений между пользователями компьютерной сети Интернет. Необходимые для проведения практики перечень основной и дополнительной литературы, перечень учебно-методического обеспечения для самостоятельной работы обучающихся, раздаточный материал и методические указания передаются студентам в электронном виде. Электронная информационно-образовательная среда КФ МГТУ им. Н.Э. Баумана обеспечивает доступ к рабочей программе практики, к изданиям электронных библиотечных систем и электронным образовательным ресурсам, указанным в рабочей программе практики, фиксацию хода образовательного процесса и результатов промежуточной аттестации по практике.

Программное обеспечение

1. Window Server CAL 2008 Russian
2. Office Professional Plus 2007 Russian
3. MS Visual Studio
4. Multisim (Electronics Workbench)

Информационные и справочные системы:

1. Информационно-справочный портал «Library.ru». http://www.library.ru.
2. Информационный портал по информационной безопасности http://www.securitylab.ru/
3. Информационный ресурс по информационной безопасности BugTraq.Ru https://bugtraq.ru/
4. Некоммерческий информационный портал, посвященный международным стандартам в области управления информационной безопасностью серии ISO 27000 http://www.iso27001security.com/
5. Официальный сайт Федеральной службы по техническому и экспортному контролю. http://fstec.ru/

10. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ

1. Помещения для самостоятельной работы обучающихся, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду.

Каждый обучающийся в период прохождения преддипломной практики обеспечен индивидуальным неограниченным доступом к полнотекстовым документам Научной Электронной Библиотеки (НЭБ) http://elibrari.ru, электронной библиотечной системы издательства «Лань» http://e.lanbook.com, электронно–библиотечной системы «Университетская библиотека онлайн» http://biblioclub.ru, электронно-библиотечной системы «IPRbooks» http://www.iprbooksshop.ru, электронно-библиотечной системы «Юрайт» https://www.biblio-online.ru, электронному каталогу библиотеки МГТУ им. Н.Э. Баумана http://library.bmstu.ru из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети «Интернет», как на территории КФ МГТУ им. Н.Э. Баумана, так и вне ее.

Обучающимся обеспечен доступ в дисплейном зале библиотеки через локальную сеть МГТУ им. Н.Э. Баумана к научным лицензионным материалам:

– полнотекстовые научные издания: IEEE/IET Electronic Library (IEL) (журналы, конференции, стандарты, книги MIT); SPIE (журналы, конференции); OSA Optical Society of America (журналы, конференции); ScienceDirect (Elsevier) (журналы, книги); OUP Oxford University Press (журналы); AIP American Institute of Physics (журналы); Science (журнал); Sage Publications (журналы); Nature (журналы); Taylor & Francis (журналы); Springer (журналы, книги); Wiley (журналы); APS American Physical Sosiety;

– научная электронная библиотека: Questel QPAT (Patent), «Консультант» (правовая БД), «КОДЕКС» (правовая БД);

– энциклопедии, словари, справочники: Encyclopedia of Medical Devices and Instrumentation;

– реферативные БД и поисковые системы: Реферативный журнал ВИНИТИ; SCOPUS; Web of Science; РИНЦ; INSPEC; MathsciNet (БД публикаций по математике).