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 ПП.ИУ6-01/19

Факультет «Информатика и управление» (ИУ-КФ)

Кафедра «Защита информации» ИУ6-КФ

ПРОГРАММА ПРАКТИКИ

Производственная практика

Вид практики

Профессиональная практика

Тип практики

для специальности 10.05.03 «Информационная безопасность автоматизированных систем»

специалиста (специализация «Анализ безопасности информационных систем»)

Автор(ы) программы:

Мазин А.В., д.т.н., доцент, MazinAV@bmstu-kaluga.ru

Калуга, 2019

Автор(ы) программы:

Мазин А.В. _____

Рецензент:
Зам. директора
АО «Калуга Астрал»

Елфимов Ю.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

Адкин 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 – профессиональная.

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 проводить анализ рисков информационной безопасности автоматизированной системы (СПК-5);

Результаты обучения при прохождении практики, соотнесенные с компетенцией		
Обучающийся должен знать:	Обучающийся должен уметь:	Обучающийся должен владеть:
- понятия риска информационной безопасности; анализа рисков информационной безопасности; управления рисками информационной безопасности; - методы анализа рисков информационной безопасности автоматизированной системы.	- применять методы анализа рисков информационной безопасности автоматизированной системы	- навыками проведения анализа рисков информационной безопасности автоматизированной системы.

- способность проводить анализ и расчет надежности средств информационной безопасности (СПК-10);

Результаты обучения при прохождении практики, соотнесенные с компетенцией		
Обучающийся должен знать:	Обучающийся должен уметь:	Обучающийся должен владеть:
- понятие надежности средств информационной безопасности; - методы анализа и расчета надежности средств информационной безопасности.	- применять методы анализа и расчета надежности средств информационной безопасности.	- навыками проведения анализа и расчета надежности средств информационной безопасности.

- 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 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 проектировании системы управления информационной безопасностью автоматизированной системы (СПК-16);

Результаты обучения при прохождении практики, соотнесенные с компетенцией		
Обучающийся должен знать:	Обучающийся должен уметь:	Обучающийся должен владеть:
- понятие системы управления информационной безопасностью автоматизированной системы; - нормативные документы по системам управления информационной безопасностью автоматизированной системы.	- разрабатывать документацию, регламентирующую функционирование системы управления информационной безопасностью автоматизированной системы.	- навыками участия в проектировании системы управления информационной безопасностью автоматизированной системы.

- способность разрабатывать средства противодействия вирусной активности, в том числе для современных поколений вирусов, поражающих мобильные программно-аппаратные комплексы и устройства связи (СПК-18);

Результаты обучения при прохождении практики, соотнесенные с компетенцией		
Обучающийся должен знать:	Обучающийся должен уметь:	Обучающийся должен владеть:
- понятия вируса, вирусной активности; - признаки вирусной активности на различных программно – аппаратных комплексах и устройствах связи.	- разрабатывать программные продукты.	- навыками разработки средств противодействия вирусной активности, в том числе для современных поколений вирусов, поражающих мобильные программно-аппаратные комплексы и устройства связи.

- способность разрабатывать и внедрять комплексы автоматизированных рабочих мест администратора информационной безопасности, в том числе для противодействия инсайдерской активности внутри защищаемого периметра (СПК-19);

Результаты обучения при прохождении практики, соотнесенные с компетенцией		
Обучающийся должен знать:	Обучающийся должен уметь:	Обучающийся должен владеть:
- понятия автоматизированного рабочего места администратора информационной безопасности, инсайдерской активности, защищаемого периметра; - требования к автоматизи-	- выполнять работы по разработке и внедрению автоматизированного рабочего места администратора информационной безопасности	- навыками разработки и внедрения комплексов автоматизированных рабочих мест администратора информационной безопасности, в том числе для противодействия инсайдерской активно-

рованным рабочим местам администратора информационной безопасности.		сти внутри защищаемого периметра.

- способность осуществлять проектирование конфигураций модулей доверенной загрузки для всех возможных типов средств защиты (СПК-20);

Результаты обучения при прохождении практики, соотнесенные с компетенцией		
Обучающийся должен знать:	Обучающийся должен уметь:	Обучающийся должен владеть:
- понятие модуля доверенной загрузки; - требования к конфигурации модулей доверенной загрузки; - принципы проектирования конфигураций модулей доверенной загрузки для всех возможных типов средств защиты.	- выполнять работы по проектированию конфигураций	- навыками осуществления проектирования конфигураций модулей доверенной загрузки для всех возможных типов средств защиты.

- 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:
- состав конструкторской, технологической и ремонтной документации на программные, технические и программно-аппаратные средства защиты	- оформлять конструкторскую, технологическую и ремонтную документацию на программные, технические и программно-аппаратные средства защиты	- навыками разработки конструкторской, технологической и ремонтной документации на программные, технические и программно-аппаратные средства защиты.

- способность участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации (СПК-25);

Результаты обучения при прохождении практики, соотнесенные с компетенцией		
Обучающийся должен знать:	Обучающийся должен уметь:	Обучающийся должен владеть:
- понятие аттестации автоматизированных систем; - нормативные документы по защите информации.	- составлять план экспериментально - исследовательских работ; - оформлять отчеты о проведенных экспериментально-исследовательских работ при аттестации.	- навыками участия в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации.

- 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 информации.	- применять средства инструментального мониторинга.	- навыками проведения инструментального мониторинга защищенности информации в автоматизированной системе и выявлять каналы утечки информации.

- способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы (СПК-29);

Результаты обучения при прохождении практики, соотнесенные с компетенцией		
Обучающийся должен знать:	Обучающийся должен уметь:	Обучающийся должен владеть:
- понятие системы управления информационной безопасностью автоматизированной системы; - требования к системе управления информационной безопасностью автоматизированной системы.	- выявлять угрозы и уязвимости для объекта информатизации; - оформлять документацию по организации информационной безопасности в автоматизированной системе.	- навыками разработки предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы.

- способность организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности (СПК-30);

Результаты обучения при прохождении практики, соотнесенные с компетенцией		
Обучающийся должен знать:	Обучающийся должен уметь:	Обучающийся должен владеть:
- требования информационной безопасности в АС; - этапы жизненного цикла автоматизированной системы (разработку, внедрение, эксплуатацию и сопровождение).	- выполнять работы по разработке, внедрению, эксплуатации и сопровождению автоматизированной системы	- навыками организации разработки, внедрения, эксплуатации и сопровождения автоматизированной системы с учетом требований информационной безопасности.

- способность разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем (СПК-31);

Результаты обучения при прохождении практики, соотнесенные с компетенцией		
Обучающийся должен знать:	Обучающийся должен уметь:	Обучающийся должен владеть:
- документы, регламентирующие работу по обеспечению информационной безопасности автоматизированных систем.	- оформлять документы в соответствии с требованиями ГОСТ.	- навыками разработки проектов документов, регламентирующих работу по обеспечению информационной безопасности автоматизирован-

		ных систем.

- способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (СПК-32);

Результаты обучения при прохождении практики, соотнесенные с компетенцией		
Обучающийся должен знать:	Обучающийся должен уметь:	Обучающийся должен владеть:
- понятие политики информационной безопасности организации, этапы ее разработки; - приемы разработки политики безопасности, контроля эффективности реализации.	- собирать информацию об информационных, материальных ресурсах, персонале предприятия; - оценивать информационные риски; - предлагать методы и средства для снижения информационных рисков.	- навыками формирования политики информационной безопасности организации и контроля эффективности ее реализации.

- способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа (СПК-33);

Результаты обучения при прохождении практики, соотнесенные с компетенцией		
Обучающийся должен знать:	Обучающийся должен уметь:	Обучающийся должен владеть:
- понятия информации ограниченного доступа, правила, процедуры, метода для защиты информации ограниченного доступа; - состав комплекса мер для защиты информации ограниченного доступа; - приемы формирования комплекса мер для защиты информации ограниченного доступа.	- формировать и оформлять документы, регламентирующие защиту информации ограниченного доступа.	- навыками формирования комплекса мер (правила, процедуры, методы) для защиты информации ограниченного доступа.

- способность принимать участие в работе комиссий по проведению специальных экспертиз предприятий промышленности на право получения лицензий по созданию средств защиты информации (СПК-34);

Результаты обучения при прохождении практики, соотнесенные с компетенцией		
Обучающийся должен знать:	Обучающийся должен уметь:	Обучающийся должен владеть:
- понятие лицензии по созданию средств защиты информации; - порядок проведения лицензирования промышленных предприятий на право получения лицензий по созданию средств защиты информации; - виды документов, оформляемых для получения лицензий по созданию средств защиты информации.	- формировать и оформлять документы на право получения лицензий по созданию средств защиты информации.	- навыками участия в работе комиссий по проведению специальных экспертиз предприятий промышленности на право получения лицензий по созданию средств защиты информации.

- способность принимать участие в работе по подготовке и проведению сертификационных испытаний средств защиты информации в составе органов по сертификации и испытательных лабораторий (СПК-35).

Результаты обучения при прохождении практики, соотнесенные с компетенцией		
Обучающийся должен знать:	Обучающийся должен уметь:	Обучающийся должен владеть:
- понятие сертификационных испытаний; - порядок проведения сертификационных испытаний средств защиты информации.	- составлять план проведения сертификационных испытаний.	- навыками участия в работе по подготовке и проведению сертификационных испытаний средств защиты информации в составе органов по сертификации и испытательных лабораторий.

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;
- выполнение проектов по созданию программ, комплексов программ, программно-аппаратных средств, баз данных, компьютерных сетей для защищенных автоматизированных систем;
- разработка систем управления информационной безопасностью автоматизированных систем;
- контроль работоспособности и эффективности применяемых средств защиты информации;
- выполнение экспериментально-исследовательских работ при сертификации средств защиты информации и аттестации автоматизированных систем;
- проведение инструментального мониторинга защищенности автоматизированных систем и анализа его результатов;
- организационно-методическое обеспечение информационной безопасности автоматизированных систем;
- организация работ по созданию, внедрению, эксплуатации и сопровождению защищенных автоматизированных систем.

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;
- системы управления информационной безопасностью 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: Учебно – технологический практикум, Теоретическая информатика, Языки программирования, Основы информационной безопасности, Теоретические основы информационной безопасности автоматизированных систем, Управление информационной безопасностью, Анализ рисков информационной безопасности, Разработка и эксплуатация защищенных автоматизированных систем.

Результаты прохождения практики необходимы как предшествующие для освоения следующих дисциплин (практик) учебного плана: Преддипломная практика, Научно-исследовательская работа.

4. ОБЪЕМ ПРАКТИКИ И ЕЕ ПРОДОЛЖИТЕЛЬНОСТЬ

	Всего	Продолжительность и объем по семестрам
		10 семестр 3 недели
Объем практики, з.е.	**3**	**3**
Объем практики, час.	108	108
Промежуточная аттестация		Зачет

5. СОДЕРЖАНИЕ ПРАКТИКИ

№ пп	Этапы практики	Час.
	10 семестр	108
5.1	Ознакомление со структурой предприятия, применяемыми средствами и методами обеспечения информационной безопасности предприятия или его конкретного подразделения	8
5.2	Участие в работах по обеспечению информационной безопасности автоматизированной системы предприятия или его подразделения	20
5.3	Участие в работах по организации системы управления информационной безопасностью автоматизированной системы предприятия или его подразделения	20
5.4	Участие в разработке средств обеспечения информационной безопасности	20
5.5	Участие в разработке документации	20
5.6	Участие в работах по проведению аттестации, лицензирования и сертификации в сфере информационной безопасности	15
5.7	Оформление отчета о проведенной работе	4
5.8	Промежуточная аттестация	1

Содержание

5.1 Ознакомление со структурой предприятия, применяемыми средствами и методами обеспечения информационной безопасности предприятия или его конкретного подразделения

Цель: сформировать первичные профессиональные умения и навыки организации разработки, внедрения, эксплуатации и сопровождения автоматизированной системы с учетом требований информационной безопасности.

Задачи: ознакомиться со структурой предприятия, ознакомиться с применяемыми на предприятии в целом или в конкретном его подразделении средствами и методами обеспечения информационной безопасности.

5.2 Участие в работах по обеспечению информационной безопасности автоматизированной системы предприятия или его подразделения

Цель: сформировать первичные профессиональные умения и навыки разработки и анализа проектных решений по обеспечению безопасности автоматизированных систем; проведения анализа и расчета надежности средств информационной безопасности; проведения инструментального мониторинга защищенности информации в автоматизированной системе и выявлять каналы утечки информации; организации разработки, внедрения, эксплуатации и сопровождения автоматизированной системы с учетом требований информационной безопасности.

Задачи: изучить существующие решения по обеспечению безопасности автоматизированной системы; провести расчет надежности применяемых средств информационной безопасности, провести инструментальный мониторинг защищенности информации в автоматизированной системе, выявление каналов утечки информации; ознакомиться с этапами разработки, внедрения, эксплуатации и сопровождения автоматизированной системы предприятия с учетом требований информационной безопасности.

5.3 Участие в организации системы управления информационной безопасностью автоматизированной системы предприятия или его подразделения

Цель: сформировать первичные профессиональные умения и навыки проведения анализа рисков информационной безопасности автоматизированной системы; участия в проектировании системы управления информационной безопасностью автоматизированной системы; предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы; формирования политики информационной безопасности организации и контроля эффективности ее реализации.

Задачи: собрать информацию об активах предприятия (или рассматриваемого структурного подразделение), угрозах и уязвимостях информационной безопасности, позволяющую оценить уровень информационных рисков; принять участие в анализе рисков ИБ; принять участие в проектировании системы управления информационной безопасностью (ИБ) автоматизированной систем (АС) или изучить структуру существующей системы управления ИБ АС; предложить возможные пути ее совершенствования; принять участие в формировании политики информационной безопасности организации или в процессе контроля эффективности ее реализации.

5.4 Участие в разработке средств обеспечения информационной безопасности

Цель: сформировать первичные профессиональные умения и навыки разработки средств противодействия вирусной активности, в том числе для современных поколений вирусов, поражающих мобильные программно-аппаратные комплексы и устройства связи; разработки и внедрения комплексов автоматизированных рабочих мест администратора информационной безопасности, в том числе для противодействия инсайдерской активности внутри защищаемого периметра; осуществления проектирования конфигураций модулей доверенной загрузки для всех возможных типов средств защиты.

Задачи: принять участие в разработке средств противодействия вирусной активности; принять участие в разработке или внедрении комплексов автоматизированных рабочих мест администратора информационной безопасности; принять участие в проектировании конфигураций модулей доверенной загрузки.

5.5 Участие в разработке документации

Цель: сформировать первичные профессиональные умения и навыки разработки конструкторской, технологической и ремонтной документации на программные, технические и программно-аппаратные средства защиты; разработки проектов документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем; формирования комплекса мер (правила, процедуры, методы) для защиты информации ограниченного доступа.

Задачи: изучить состав конструкторской, технологической и ремонтной документации на программные, технические и программно-аппаратные средства защиты, применяемые на предприятии; изучить состав и (или) принять участие в разработке документации, регламентирующей работы по обеспечению информационной безопасности рассматриваемой автоматизированной системы; изучить существующий комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа, сделать предложения по его совершенствованию или принять участие в его формировании.

5.6 Участие в работах по проведению аттестации, лицензирования и сертификации в сфере информационной безопасности

Цель: сформировать первичные профессиональные умения и навыки участия в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации, участия в работе комиссий по проведению специальных экспертиз предприятий промышленности на право получения лицензий по созданию средств защиты информации, участия в работе по подготовке и проведению сертификационных испытаний средств защиты информации в составе органов по сертификации и испытательных лабораторий.

Задачи: принять участие в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации; принять участие в работе комиссий по проведению специальных экспертиз предприятий промышленности на право получения лицензий по созданию средств защиты информации; принять участие в работе по подготовке и проведению сертификационных испытаний средств защиты информации в составе органов по сертификации и испытательных лабораторий.

5.7 Оформление отчета о проведенной работе

Цель: сформировать первичные профессиональные умения и навыки применения достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах.

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

5.8 Промежуточная аттестация

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

6. ФОРМА ОТЧЕТНОСТИ ПО ПРАКТИКЕ

Форма отчетности по практике – письменный отчет.

Форма промежуточной аттестации по практике – зачет с выставлением дифференцированной оценки.

Структура отчета студента по практике:

– Титульный лист. На титульном листе указывается официальное название МГТУ им. Н.Э. Баумана, факультета, выпускающей кафедры, ФИО студента, группа, название практики, должности и ФИО руководителя практики от МГТУ имени Н.Э. Баумана, должность и ФИО руководителя практики от предприятия – базы практики.
– Содержание (оглавление)
– Введение. В разделе должны быть приведены цели и задачи практики.
– Основная часть. В разделе приводится описание выполненных студентом работ в соответствии с целями и задачами практики и индивидуальным заданием, приводятся полученные студентом результаты.
– Заключение. В разделе должны быть представлены выводы по результатам практики.
– Список использованных источников.
– Приложения.

Сброшюрованный отчет подписывается руководителями практики.

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] / А.В. Васильков, А.А. Васильков, И.А. Васильков. – М.: Изд-во «Форум», 2013. – 528 с.

Дополнительная литература

1. Денисов, В.В. Анализ состояния защиты данных в информационных системах [Электронный ресурс]: учебно-методическое пособие / В.В. Денисов. – Новосибирск: Изд-во НГТУ, 2012. – 52 с. – URL: http://biblioclub.ru/index.php?page=book&id=228844

2. Кияев, В.И., Граничин, О.Н. Безопасность информационных систем [Электронный ресурс]: курс лекций / В.И. Кияев, О.Н. Граничин. - М.: Национальный Открытый Университет «ИНТУИТ», 2016. - 192 с. – URL: https://biblioclub.ru/index.php?page=book_red&id=429032.

3. Фридман, А.Л. Язык **программирования** Си++ [Электронный ресурс]: учебное пособие/ А.Л. Фридман. – Изд. 2-е, испр. – Москва: Интернет-Университет Информационных Технологий, 2004. – 262 с. – URL: http://biblioclub.ru/index.php?page=book&id=233058

4. Царев, Р.Ю. Программирование на языке Си [Электронный ресурс]: учебное пособие / Р.Ю. Царев. – Красноярск: Сибирский федеральный университет, 2014. – 108 с. – на англ. языке – URL: http://biblioclub.ru/index.php?page=book&id=364601

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

Информационные и справочные системы:

1. Информационно-справочный портал «Library.ru». http://www.library.ru.
2. Научное информационное пространство «Соционет». http://www.socionet.ru.

3. Некоммерческая организация защиты авторских прав Creative Commons. http://creativecommons.org.

4 Евразийская патентная информационная система (ЕАПАТИС). http://eapatis.com.

5. Федеральная служба по интеллектуальной собственности (Роспатент). http://www.rupto.ru.

6. Всемирная организация интеллектуальной собственности. http://www.wipo.int/portal/ru.

7. Портал «Интеллектуальная собственность. Авторское право и смежные права. Патентное право. Регистрация прав». http://www.copyright.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.

2. Для успешного прохождения практики обучающемуся на предприятии в отделе прохождения практики должно быть организовано место (стол, стул, ПК), открыт доступ к документации отдела, предоставлена возможность посещения подразделений предприятия, участвующих в процессе обеспечения информационной безопасности автоматизированной системы предприятия.