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.ИУ6-18/19

Факультет «Информатика и управление» (ИУ-КФ)

Кафедра «Защита информации» ИУ6-КФ

ПРОГРАММА ПРАКТИКИ

Производственная практика

Вид практики

Технологическая практика

Тип практики

для специальности 10.05.03 «Информационная безопасность автоматизированных систем»

специалиста (специализация «Анализ безопасности информационных систем»)

Автор(ы) программы:

Лачихина А.Б., к.т.н., доцент, LachkhinaAB@bmstu-kaluga.ru

Калуга, 2019

Автор(ы) программы:

Лачихина А.Б. _____

Рецензент:
Директор по маркетингу, сбыту и специальным видам работ
ЗАО НПФ «Сигма»

Герасимов П.Н. _____

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 – технологическая.

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 создавать и исследовать модели автоматизированных систем (СПК-2);

Результаты обучения при прохождении практики, соотнесенные с компетенцией		
Обучающийся должен знать:	Обучающийся должен уметь:	Обучающийся должен владеть:
- понятия автоматизированной системы, модели, модели автоматизированной системы; - подходы к разработке и исследованию модели автоматизированной системы	- строить модель автоматизированной системы;	- навыками создания и исследования модели автоматизированных систем.

- способность проводить анализ защищенности автоматизированных систем (СПК-3);

Результаты обучения при прохождении практики, соотнесенные с компетенцией		
Обучающийся должен знать:	Обучающийся должен уметь:	Обучающийся должен владеть:
- понятие информационной безопасности в автоматизированной системе; - методы оценки защищенности.	- применять методы оценки защищенности.	- навыками проведения анализа защищенности автоматизированных систем.

- способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности (СПК-6);

Результаты обучения при прохождении практики, соотнесенные с компетенцией		
Обучающийся должен знать:	Обучающийся должен уметь:	Обучающийся должен владеть:
- понятие автоматизированной системы; - варианты применения автоматизированных систем. в различных областях деятельности.	- анализировать и выбирать решения по применению автоматизированных систем.	- навыками проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности.

- способность разрабатывать формальные модели управления доступом при проектировании, реализации и внедрении автоматизированных систем в защищенном исполнении (СПК-8);

Результаты обучения при прохождении практики, соотнесенные с компетенцией		
Обучающийся должен знать:	Обучающийся должен уметь:	Обучающийся должен владеть:
- процедуры управления доступом; - существующие формальные модели управления доступом; - механизмы разграничения доступа к файлам и каталогам, идентификации и аутентификации пользователей современных ОС.	- выбирать механизмы управления доступом для конкретных задач и этапов жизненного цикла автоматизированных систем.	- навыками разработки формальных моделей управления доступом при проектировании, реализации и внедрении автоматизированных систем в защищенном исполнении.

- 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 политику информационной безопасности автоматизированной системы (СПК-15);

Результаты обучения при прохождении практики, соотнесенные с компетенцией		
Обучающийся должен знать:	Обучающийся должен уметь:	Обучающийся должен владеть:
- понятия политики безопасности; - основные разделы политик	- разрабатывать политику информационной безопасности.	- навыками разработки политики информационной безопасности автоматизирован-

безопасности.		ной системы.

- 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.

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

- научно-исследовательская;
- проектно-конструкторская деятельность;
- контрольно-аналитическая.

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

– выполнение проектов по созданию программ, комплексов программ, программно-аппаратных средств, баз данных, компьютерных сетей для защищенных автоматизированных систем;
– контроль работоспособности и эффективности применяемых средств защиты информации.

Объектами профессиональной деятельности выпускников, успешно прошедших практику в составе образовательной программы, являются:
– информационные технологии, формирующие информационную инфраструктуру в условиях существования угроз в информационной сфере и задействующие информационно-технологические ресурсы, подлежащие защите.

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, Ознакомительная практика, Теоретическая информатика, Языки программирования, Электроника и схемотехника, Аппаратные средства вычислительной техники.
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
		8 семестр 3 недели
Объем практики, з.е.	**4**	**4**
Объем практики, час.	144	144
Промежуточная аттестация		Зачет

5. СОДЕРЖАНИЕ ПРАКТИКИ

№ пп	Этапы практики	Час.
	8 семестр	144
5.1	Разработка или изучение уже существующей модели автоматизированной системы конкретного подразделения предприятия	6
5.2	Анализ защищенности автоматизированной системы конкретного подразделения предприятия	6
5.3	Постановка и решение задачи оптимального выбора средств защиты информации	6
5.4	Выбор решений по обеспечению эффективного применения автоматизированной системы конкретного подразделения предприятия	6
5.5	Разработка формальной модели управления доступом автоматизированной системы конкретного подразделения предприятия	6
5.6	Участие в разработке политики информационной безопасности автоматизированной системы конкретного подразделения предприятия	12

5.7	Изучение технического задания на разработку аппаратно- программного, аппаратного или программного средства обеспечения информационной безопасности	6
5.8	Участие в проектировании аппаратно- программного, аппаратного или программного средства обеспечения информационной безопасности	24
5.9	Реализация проекта (части проекта) аппаратно- программного, аппаратного или программного средства обеспечения информационной безопасности	42
5.10	Проведение контрольной проверки работоспособности разработанного средства защиты информации	24
5.11	Оформление отчета о проведенной работе	5
5.12	Промежуточная аттестация	1

Содержание

5.1 Разработка или изучение уже существующей модели автоматизированной системы конкретного подразделения предприятия

Цель: сформировать первичные профессиональные умения и навыки создания и исследования модели автоматизированных систем.

Задачи: изучить существующую или разработать новую модель автоматизированной систем подразделения предприятия.

5.2 Анализ защищенности автоматизированной системы конкретного подразделения предприятия

Цель: сформировать первичные профессиональные умения и навыки проведения анализа защищенности автоматизированных систем.

Задачи: определить, к какой категории защищенности относится рассматриваемая АС; оценить соответствие применяемых средств защиты информации требованиям, предъявляемым к АС данного класса.

5.3 Постановка и решение задачи оптимального выбора средств защиты информации

Цель: сформировать первичные профессиональные умения и навыки осуществления математической постановки задачи и ее решения современными оптимизационными методами для оптимального выбора средств защиты информации при ограничениях на их стоимость, габариты, энергопотребление и др.

Задачи: сформулировать задачу выбора средств защиты информации при ограничениях на их определенные параметры для рассматриваемой АС, записать математическую постановку задачи и решить ее.

5.4 Выбор решений по обеспечению эффективного применения автоматизированной системы конкретного подразделения предприятия

Цель: сформировать первичные профессиональные умения и навыки проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности.

Задачи: провести анализ набора функций, выполняемых рассматриваемой автоматизированной системой, режима работы системы, применяемых средств автоматизации; сделать вывод о рациональности набора выполняемых функций; предложить свой вариант более эффективного на ваш взгляд применения автоматизированной системы в данном подразделения предприятия

5.5 Разработка формальной модели управления доступом автоматизированной системы конкретного подразделения предприятия

Цель: сформировать первичные профессиональные умения и навыки разработки формальных моделей управления доступом при проектировании, реализации и внедрении автоматизированных систем в защищенном исполнении.

Задачи: на основе класса защищенности АС предложить тип формальной модели управления доступом для рассматриваемой АС; разработать подробное описание формальной модели управления доступом для рассматриваемой АС.

5.6 Участие в разработке политики информационной безопасности автоматизированной системы конкретного подразделения предприятия

Цель: сформировать первичные профессиональные умения и навыки разработки политики информационной безопасности автоматизированной системы.

Задачи: изучить существующую на предприятии политику безопасности (при ее наличии); разработать политику безопасности для конкретного подразделения предприятия или конкретной подсистемы рассматриваемой АС.

5.7 Изучение технического задания на разработку аппаратно- программного, аппаратного или программного средства обеспечения информационной безопасности

Цель: сформировать первичные профессиональные умения и навыки осуществления разработки аппаратно – программных средств обеспечения информационной безопасности.

Задачи: провести анализ технического задания на разработку средства обеспечения информационной безопасности, определить требования к функциям, которые должно выполнять средство обеспечения ИБ.

5.8 Проектирование аппаратно- программного, аппаратного или программного средства обеспечения информационной безопасности

Цель: сформировать первичные профессиональные умения и навыки осуществления разработки аппаратно – программных средств обеспечения информационной безопасности.

Задачи: разработать структуру проектируемого средства обеспечения ИБ, разработать необходимые схемы проектируемого средства обеспечения ИБ, выбрать средства реализации.

5.9 Реализация проекта аппаратно- программного, аппаратного или программного средства обеспечения информационной безопасности

Цель: сформировать первичные профессиональные умения и навыки осуществления разработки аппаратно – программных средств обеспечения информационной безопасности.

Задачи: реализовать разработанный проект средства обеспечения информационной безопасности.

5.10 Проведение контрольной проверки работоспособности разработанного средства защиты информации

Цель: сформировать первичные профессиональные умения и навыки проведения контрольных проверок работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации.

Задача: разработать план проведения контрольной проверки работоспособности разработанного средства обеспечения информационной безопасности; провести проверку; оценить результаты проведенной проверки работоспособности; оформить отчет о проведенной проверке работоспособности.

5.11 Оформление отчета о проведенной работе

Цель: сформировать первичные профессиональные умения и навыки осуществления разработки аппаратно – программных средств обеспечения информационной безопасности и про-

ведения 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.

5.12 Промежуточная аттестация

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

5 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.

6 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.

7 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 : 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. (УМО по университетскому политехническому образованию) 100 экз.

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.

8 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/

9 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.