МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

УТВЕРЖДАЮ:

Директор ИТТСУ

П.Ф. Бестемьянов

«26» июня 2019 г.

Кафедра: Управление и защита информации
Авторы: Алексеев Виктор Михайлович, доктор технических наук, профессор

ПРОГРАММА ПРАКТИКИ

Научно-исследовательская работа

Специальность:	10.05.01 Компьютерная безопасность
Специализация:	Информационная безопасность объектов информатизации на базе компьютерных систем
Квалификация выпускника:	Специалист по защите информации
Форма обучения:	Очная
Год начала обучения:	2019

Одобрено на заседании Учебно-методической комиссии	Одобрено на заседании кафедры
Протокол № 10 «25» июня 2019 г. Председатель учебно-методической комиссии _____ С.В. Володин	Протокол № 21 «24» июня 2019 г. Заведующий кафедрой _____ Л.А. Баранов

Москва 2019

1. Цели практики

Целями практики являются получение и развитие компетенций научно-исследовательской деятельности.
В соответствии с целями ОП ВО «Научно-исследовательская работа» направлена формирование у будущих специалистов умения самостоятельно вести научно-исследовательскую деятельность и позволяет:
- повысить качество подготовки выпускников в университете как едином учебно-научно-производственном комплексе через освоение студентами в процессе обучения по учебным планам и сверх них основ профессионально-творческой деятельности;
- закрепление и углубление теоретической подготовки обучающегося, приобретение им практических навыков и компетенций, а также опыта самостоятельной профессиональной деятельности.

2. Задачи практики

Задачами практики являются :
- способности к самостоятельному обучению новым методам исследования, к изменению научного и научно-производственного профиля своей профессиональной деятельности;
- способности самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, непосредственно не связанных со сферой деятельности;
- способности проектировать сложные системы и комплексы управления информационной безопасностью с учетом особенностей объектов защиты;
- способности разработать программы и методики испытаний, организовать тестирование и отладку программно- аппаратных, криптографических и технических систем и средств обеспечения информационной безопасности.
НИР выполняется каждым студентом индивидуально на тему, выдаваемую научным руководителем (или выбираемую совместно с научным руководителем) и утверждаемую кафедрой. Тема НИР должна быть актуальной и соответствовать специальности и уровню учебной подготовки студентов. Работа должна обладать тематической и логической завершенностью. Работа должна быть направлена на решение теоретической, методической либо практической задачи, результаты которой могут принести пользу для деятельности организаций, предприятий, учреждений, ведущих работы по направлению «Информационная безопасность», в научно-исследовательских, опытно-конструкторских либо учебно-методических работах, выполняемых на кафедре "Управление и защита информации".
Темы для научно-исследовательской работы:
Построение систем цифровых водяных знаков ЦВЗ в системах документооборота.
Цифровая подпись на основе использования эллиптических кривых в компьютерных системах.
Методы стеганографии для защиты информации в компьютерных системах.
Разработка лабораторных работ на тему «Криптография с открытым ключом».
Методы квантовой криптографии для защиты информации в компьютерных

системах.
Разработка и применение программно-аппаратных и инженерно-технических средств защиты информации, обеспечение информационной безопасности автоматизированных систем для высокоскоростного транспорта.
Разработка модели безопасности и мониторинга компьютерных сетей предприятий промышленного комплекса России.
Разработка комплексной системы защиты информации в корпоративных сетях.
Разработка политики безопасности в беспроводных сетях (WLAN).
Построение Web-приложений с учетом возможных методов нападения.
Разработка системы мониторинга информационной безопасности Web-приложений.
Защита информации и приложений с использованием удостоверяющих центров.
Разработка систем мониторинга компьютерной сети на основе методов распознавания.
Методы анализа протоколов для нахождения атак в сетевом трафике.
Методы анализа поведения пользователей в сети и выявление вредоносного поведения.
Разработка и анализ антивирусной защиты компьютерных сетей.
Разработка методов защиты почтовых приложений от спама.
Защита персональных данных и коммерческой тайны в компьютерных системах.
Разработка защиты информации в распределенных компьютерных системах.
Разработка защищённых баз данных.
Разработка системы информационной безопасности банков.

3. Место практики в структуре ОП ВО

Научно-исследовательская работа относится к Блоку 2 «Практики, в том числе научно-исследовательская работа (НИР)», части «Производственная практика».
Научно-исследовательская работа выполняется на шестом курсе в семестре "В" в течение 6 недель (с 1 сентября по 12 октября).
Научно-исследовательская работа специалистов по защите информации по направлению 10.05.01 – "Компьютерная безопасность. Информационная безопасность объектов информатизации на базе компьютерных систем" базируется на следующих дисциплинах:
- «Модели безопасности компьютерных систем»;
- «Теоретико-числовые методы в криптографии»;
- «Криптографические интефейсы»;
- «Защита информации в интернет и интранет системах».

Для успешного освоения научно-исследовательской работы специалист должен:
- знать основные решения в области информационной безопасности;
- владеть современными методами построения анализаторов и языками программирования;
- уметь анализировать и обобщать полученные результаты.

Основные положения научно-исследовательской работы будут использованы при подготовке выпускной квалификационной работы - дипломного проекта.

4. Тип практики, формы и способы ее проведения

Вид практики: производственная
Тип практики: научно-исследовательская работа
Форма проведения практики: непрерывная
Способ проведения практики: стационарная; выездная.

НИР специалистов по направлению 10.05.01 по способу организации практики может быть как стационарной, так и выездной (в случае наличиия у студента целевого направления) и проводится на 6 курсе в семестре В (11 семестр).
Практика реализуется в форме выполнения научно-исследовательской работы (НИР), которая направлена на проведение научных исследований или выполнение программно-технических разработок.
НИР может проводиться как в сторонних организациях, основная деятельность которых предопределяет наличие объектов и видов профессиональной деятельности выпускников по данной специальности (специализации), так и на базе лабораторий РУТ (МИИТ).

5. Организация и руководство практикой

Организация НИР направлена на обеспечение непрерывности и последовательности овладения обучающимися профессиональной деятельностью и на сбор исходных данных и других материалов, необходимых для выполнения выпускной квалификационной работы – дипломного проекта. Сроки проведения НИР установлены в соответствии с учебным планом, календарным учебным графиком и с учетом требований ФГОС ВО.
НИР осуществляется на базе сторонних предприятий, осуществляющих деятельность, соответствующих видам профессиональной деятельности, указанным в ФГОС ВО. НИР осуществляется непрерывно, т.е. в календарном учебном плане для реализации НИР выделено 6 недель.
Для руководства НИР, проводимой в учреждениях, организациях или компаниях назначаются руководители практики от кафедры и от предприятия.
Руководитель НИР от кафедры:
- устанавливает связь с руководителем практики от предприятия и совместно с ним составляет рабочий план проведения практики и выбирает тематику индивидуальных заданий;
- несет ответственность совместно с руководителем практики от предприятия за соблюдением сроков практики и ее содержанием;
- оказывает методическую помощь обучающимся при выполнении ими индивидуальных заданий и в подборе исходных данных и других материалов для выпускной квалификационной работы;
- оценивает результаты выполнения программы НИР.

6. Перечень планируемых результатов обучения при прохождении практики, соотнесенных с планируемыми результатами освоения ОП

№ п/п	Индекс и содержание компетенции	Ожидаемые результаты

1	2	3
1	ПКО-1 Способен принимать участие в теоретических и экспериментальных исследованиях систем защиты информации, проводить научно-исследовательские работы по оценке защищенности информации в компьютерных системах	ПКО-1.1 Участвует в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах. ПКО-1.2 Изучает и анализирует отечественный и зарубежный опыт по проблемам компьютерной безопасности. ПКО-1.3 Участвует в проведении экспериментально-исследовательских работ при сертификации средств защиты информации.
2	ПКО-2 Способен применять математические методы в области компьютерной безопасности	ПКО-2.1 Проводит анализ и разрабатывает под руководством квалифицированного специалиста математические модели безопасности компьютерных систем. ПКО-2.2 Применяет специальные математические методы, включая криптографические, для анализа и разработки защищенных компьютерных систем. ПКО-2.3 Применяет решения на основе специальных математических методов для обеспечения защищенной передачи данных в современных компьютерных сетях.
3	ПКО-3 Способен проводить анализ исходных данных и формировать требования к компонентам и методам при проектировании подсистем и средств обеспечения информационной безопасности	ПКО-3.1 Изучает и обобщает опыт работы различных учреждении?, организации? и предприятии? в области повышения эффективности защиты информации. ПКО-3.2 Формирует требования по защите информации, включая использование математического аппарата для решения прикладных задач. ПКО-3.3 Составляет планы этапов проведения научно-исследовательских и опытно- конструкторских работ. ПКО-3.4 Разрабатывает и анализирует структурные и функциональные схемы защищенных компьютерных систем в сфере профессиональной деятельности.
4	ПКО-4 Способен участвовать в разработке подсистемы информационной безопасности компьютерной (в том числе автоматизированной) системы включая разработку программно-аппаратных средств защиты информации, защищенных операционных систем, систем управления базами данных, компьютерных сетей, систем антивирусной защиты, средств криптографической защиты информации	ПКО-4.1 Осуществляет рациональный выбор технологии, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасности, создаваемых защищенных компьютерных систем в сфере профессиональной деятельности. ПКО-4.2 Проектирует и разрабатывает компоненты защищенных автоматизированных систем в сфере профессиональной деятельности.
5	ПКО-5 Способен участвовать в работах по проектированию и реализации комплексного подхода к обеспечению информационной безопасности объекта защиты	ПКО-5.1 Принимает участие в формировании политики информационной безопасности, ее реализации и контроле выполнения. ПКО-5.2 Формирует, организует и поддерживает комплекс мер по обеспечению информационной безопасности.

№ п/п	Индекс и содержание компетенции	Ожидаемые результаты
1	2	3
6	ПКО-6 Способен проводить оценку эффективности реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	ПКО-6.1 Подбирает методики и инструментарий, определяет критерии и осуществляет проверку эффективности систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации.
7	ПКО-7 Способен проводить анализ информационной безопасности объектов и систем, принимать участие в организации и сопровождении аттестации объекта информатизации на предмет соответствия требованиям защиты информации	ПКО-7.1 Проводит анализ безопасности компьютерных систем, в том числе с использованием методов моделирования, на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности. ПКО-7.2 Участвует в проведении экспериментально-исследовательских работ при аттестации объектов с учетом требовании? к уровню защищенности компьютерной системы. ПКО-7.3 Вырабатывает рекомендации в связи с проведенным анализом безопасности, в том числе для принятия решения о повторной аттестации компьютерной системы (в том числе автоматизированных систем), предложения по устранению выявленных уязвимостей.
8	ПКО-8 Способен проводить инструментальный мониторинг защищенности компьютерных систем	ПКО-8.1 Анализирует защищенность компьютерных систем с использованием сканеров безопасности. ПКО-8.2 Анализирует защищенность сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем.
9	ПКР-3 Способен принимать участие в разработке проектных решений по защите информации в автоматизированных системах	ПКР-3.1 Участвует в разработке проектных решений по защите информации в автоматизированных системах высокоскоростного транспорта. ПКР-3.2 Участвует в разработке проектных решений по защите информации в беспилотных автоматизированных системах.
10	ПКР-4 Способен разрабатывать программные и программно-аппаратные средства для систем защиты информации автоматизированных систем	ПКР-4.1 Разрабатывает программные средства для систем защиты информации автоматизированных систем высокоскоростного транспорта. ПКР-4.2 Разрабатывает программные средства для систем защиты информации автоматизированных систем в беспилотных автоматизированных системах.
11	ПКР-5 Способен проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных	ПКР-5.1 Проводит сравнительный анализ программно-аппаратных средств защиты информации с учетом современных и перспективных математических методов защиты информации. ПКР-5.2 Делает обоснованный выбор программно-

№ п/п	Индекс и содержание компетенции	Ожидаемые результаты
1	2	3
	средств защиты информации с учетом современных и перспективных математических методов защиты информации	аппаратных средств защиты информации.
12	ПКР-6 Способен принимать участие в разработке архитектуры системы защиты информации автоматизированной системы	ПКР-6.1 Участвует в разработке архитектуры системы защиты информации автоматизированных систем высокоскоростного транспорта. ПКР-6.2 Участвует в разработке архитектуры системы защиты информации беспилотных автоматизированных систем.
13	ПКР-7 Способен разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации	ПКР-7.1 Разрабатывает математические модели процессов, возникающих при работе программно-аппаратных средств защиты информации. ПКР-7.2 Анализирует математические модели процессов, возникающих при работе программно-аппаратных средств защиты информации. ПКР-7.3 Обосновывает адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации.
14	ПКР-8 Способен подготовить обоснование необходимости защиты информации в автоматизированной системе	ПКР-8.1 Проводит анализ уязвимости и устанавливает необходимые средства защиты информации для технологической базы автоматизированных систем высокоскоростного транспорта. ПКР-8.2 Проводит анализ уязвимости и устанавливает необходимые средства защиты информации для технологической базы беспилотных автоматизированных систем.

7. Объем, структура и содержание практики, формы отчетности

Общая трудоемкость практики составляет 9 зачетных единиц, 6 недель / 324 часов.

Содержание практики, структурированное по разделам (этапам)

№ п/п	Разделы (этапы) практики	Виды деятельности студентов в ходе практики, включая самостоятельную работу студентов и трудоемкость (в часах)				Формы текущего контроля
		Зет	Часов			
			Все-го	Практичес-кая работа	Самостоятельная работа	
1	2	3	4	5	6	7
1.	Этап: Постановка цели и задач исследований	0,22	8	5	3	Проверка получения всеми студентами индиви

№ п/п	Разделы (этапы) практики	Виды деятельности студентов в ходе практики, включая самостоятельную работу студентов и трудоемкость (в часах)				Формы текущего контроля
		Зет	Часов			
			Все-го	Практичес-кая работа	Самостоя те-льная работа	
1	2	3	4	5	6	7
						дуальных заданий научно-технического характера в форме собеседования
2.	Этап: Рациональные приемы поиска научно - технической информации	0,44	16	10	6	Отчет по НИР
3.	Этап: Исследования в области защиты информации, связанные с темой дипломной работы	8,33	300	165	135	Защита отчета по НИР ЗаО
	Всего:		324	180	144	

Форма отчётности: Форма отчетности по практике: отчет по НИР.

8. Перечень учебной литературы и ресурсов сети "интернет", необходимых для проведения практики

8.1. Основная литература

№ п\п	Наименование	Авторы	Год и место издания. Место доступа	Используется при изучении разделов, номера страниц
1.	Функциональная надежность информационных систем	Шубинский И. Б.	2012, Журнал Надежность. НТБ МИИТ	Все разделы
2.	Прикладные информационные системы управления надежностью, безопасностью, рисками и ресурсами на железнодорожном транспорте	Замышляев А.М.	2013, Надежность. НТБ МИИТ	Все разделы
3.	Структурная надежность информационных систем	Шубинский И. Б.	2012, Журнал Надежность.	Все разделы

№ п\п	Наименование	Авторы	Год и место издания. Место доступа	Используется при изучении разделов, номера страниц
			НТБ МИИТ	
4.	ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования	-	2013, Стандартинформ. НТБ МИИТ	Все разделы
5.	ГОСТ Р 53113.2-2009 Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов	-	2012, Стандартинформ. НТБ МИИТ	Все разделы
6.	ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель	-	2012, Стандартинформ. НТБ МИИТ	Все разделы

8.2. Дополнительная литература

№ п\п	Наименование	Авторы	Год и место издания. Место доступа	Используется при изучении разделов, номера страниц
1.	Информатизация на железнодорожном транспорте. История и современность	В.С. Наговицын, Э.С. Поддавашкин, И.В. Харланович, Ю.С. Хандкаров; Под ред. И.В. Харлановича	2005, ВЕЧЕ. НТБ (БР.); НТБ (фб.)	Все разделы
2.	Сети передачи данных информационных систем железнодорожного траспорта на базе коммутаторов и маршрутизаторов CISCO	Васин В.В.	2005, Маршрут. НТБ МИИТ	Все разделы
3.	ГОСТ Р ИСО/МЭК ТО 19791-2008 Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем	-	2013, Стандартинформ. НТБ МИИТ	Все разделы
4.	Информационная безопасность и защита информации в корпоративных сетях	В.В. Яковлев, А.А. Корниенко	2002, УМК МПС России. НТБ (уч.4); НТБ	Все разделы

№ п\п	Наименование	Авторы	Год и место издания. Место доступа	Используется при изучении разделов, номера страниц
	железнодорожного транспорта		(фб.); НТБ (чз.1)	

8.3. Ресурсы сети "Интернет"

Интернет-ресурсы
http://library.miit.ru/ - электронно-библиотечная система Научно-технической библиотеки МИИТ.
http://elibrary.ru/ - научно-электронная библиотека
Сайт ФСТЭК России: http://fstec.ru
Сайт Управление безопасностью: http://www.iso27000.ru/standarty/gost-r-nacionalnye-standarty-rossiiskoi-federacii-v-oblasti-zaschity-informacii
Периодические издания:
Журналы: Мир транспорта, Наука и техника транспорта.

9. Образовательные технологии

а) образовательные и научно-производственные технологии НИР:
- мультимедийные технологии, при которых ознакомительные лекции и инструктаж специалистов во время НИР проводятся в помещениях, оборудованных экраном, видеопроектором, персональными компьютерами (Это позволяет руководителям и специалистам предприятия (организации) экономить время, затрачиваемое на изложение необходимого материала и увеличить его объем);
- дистанционная форма консультаций во время прохождения конкретных этапов научно-исследовательской работы и подготовки отчета с использованием сети Интернета;
- компьютерные технологии и программные продукты, необходимые для сбора, систематизации результатов НИР и проведения расчетов;
б) научно-исследовательские технологии:
- системный анализ методов, моделей и средств защиты информации предметной области исследований;
- экспериментальные исследования и оценка эффективности внедрения информационного и программного обеспечения защиты компьютерных систем в предметной области дипломного проекта.

В процессе прохождения НИР, в зависимости от видов выполняемых производственных заданий по информационной безопасности на предприятиях или компаниях рекомендуется использовать следующие научно-исследовательские и научно-производственные технологии:
- технологии компаний CISCO и «Информзащита» в части аппаратных и программно-аппаратных средств защиты информации;
- технология антивирусной защиты систем и сетей;
- технология защиты от утечки информации персональной и конфиденциальной

информации КС;
- технологии защиты от хакерских атак компании Safen Soft.

10. Перечень информационных технологий, программного обеспечения и информационных справочных систем, используемых при проведении практики

Программное обеспечение для выполнения научно-исследовательской работы специалистами поспециальности 10.05.01:
- пакет программ packet tracker;
- пакет программ vpn os unix;
- среда визуального программирования Delphi, C#, VisualBasic.
- программно-аппартные комплекс ip-телефонии на базе unix.

Для освоения НИР целесообразно использовать программное обеспечение «Лаборатории Касперского» (http://writelist.kaspersy.com) и программное обеспечение от различных угроз информационной безопасности компанииSafen Soft (http://www.safensoft/.ru), а также базу научно-технической информации ВИНИТИ РАН.
http://www.itsec.ru - портал информационная безопасность
http://www.fstec.ru – сервер ФСТЭК

11. Материально-техническая база, необходимая для проведения практики

В соответствии с профилем специализации «Информационная безопасность объектов информатизации на базе компьютерных систем» для проведения НИР необходимо следующее материально-техническое обеспечение:
- лаборатории и специально оборудованные кабинеты кафедры «Управление и защита информации»:
Для проведения научно-исследовательской работы предназначены:
а) лаборатория технических средств и систем автоматизации (ауд. 4326) – стенды для изучения методов защиты информации;
б) лаборатория технических средств и систем автоматизации (ауд. 4325), в которых установлены сервера для эмуляции работы центра и филиала, с реализацией различных защитных механизмов.
При прохождении НИР на предприятии должна быть материально-техническая база, удовлетворяющая специфику направления подготовки специалиста по защите информации.
В процессе прохождения НИР, при необходимости, может использоваться научная электронная библиотека «Веда» (info@beb.ua-ru.net).