МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Декан факультета информационных технологий

_____ Филиппович А.Ю.

"01" сентября 2019 г.

РАБОЧАЯ ПРОГРАММА
Научно-исследовательская работа

Направление подготовки

10.05.03 «Информационная безопасность автоматизированных систем»

Образовательная программа (профиль подготовки)

«Обеспечение информационной безопасности распределенных информационных систем»

Квалификация выпускника

Специалист

Форма обучения

Очная

Год приема - 2019

Москва 2019 г.

1. Цели практики

К **основным целям** освоения научно-исследовательской работы следует отнести:

- закрепление и углубление теоретических знаний, полученных студентами при изучении дисциплин профессионального цикла и дисциплин специализации при исследовании системы информационной безопасности на предприятии;
- приобретение и развитие необходимых практических умений и навыков при исследовании системы информационной безопасности на предприятии в соответствии с требованиями к уровню подготовки выпускника.

2. Задачи практики

К **основным задачам** освоения научно-исследовательской работы следует отнести:

- получение практических навыков исследования средств защиты информационно-технологических ресурсов автоматизированной системы на предприятии;
- овладение методов и средств, связанных с реализацией частных политик информационной безопасности автоматизированной системы,
- осуществление мониторинга и аудита безопасности автоматизированной системы на предприятии.

3. Место практики в структуре программы

Научно-исследовательская работа относится к базовой части блока 2 «Практики, в том числе, научно-исследовательская работа (НИР)» основной образовательной программы.

Данная практика является предшествующей для выполнения выпускной квалификационной работы.

4. Тип, вид, способ и формы проведения практики

Тип и вид практики –научно-исследовательская, стационарная.

Способ и форма проведения практики – непрерывно.

5. Место и время проведения практики

Практика проводится в сторонних учреждениях, организациях и предприятиях любых организационно-правовых форм, основная деятельность которых предопределяет наличие объектов и видов профессиональной деятельности выпускников по данной специальности (специализации) или на кафедрах и в лабораториях вуза, обладающих необходимым кадровым и научно-техническим потенциалом.

Практика проводится в 10 семестре на базе предприятий требуемого профиля (4 недели).

6. Компетенции обучающегося, формируемые в результате прохождения практики

В результате освоения научно-исследовательской практики у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Код компетенции	**В результате освоения образовательной программы обучающийся должен обладать**	**Перечень планируемых результатов обучения по практике**
ПК-1	способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке;	**уметь:** - осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке;
ПК-2	способностью создавать и исследовать модели автоматизированных систем;	**знать:** - модели автоматизированных систем; **уметь:** -проводить анализ защищенности автоматизированных систем **владеть:** -методами создания моделей автоматизированных систем;
ПК-3	способностью проводить анализ защищенности автоматизированных систем;	**уметь:** - проводить анализ защищенности автоматизированных систем; **владеть:** - инструментальными средствами анализа защищенности автоматизированных систем;
ПК-4	способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы;	**уметь:** - разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы
ПК-5	способностью проводить анализ рисков информационной безопасности автоматизированной системы;	**уметь:** - проводить анализ рисков информационной безопасности автоматизированной системы; **владеть:** - методами анализа рисков информационной безопасности автоматизированной системы;

ПК-6	способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности;	**уметь:** - проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности;
ПК-7	способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ;	**уметь:** - разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ;

7. Структура и содержание практики

Общая трудоемкость практики составляет 6 зачетных единицы, 316 часов.

№ п/п	Разделы (этапы) практики	Виды работ на практике, включая самостоятельную работу студентов и трудоемкость (в зачетных единицах, часах)			Формы текущего контроля
		Виды работ	ЗЕ	час	
1	Модели автоматизированной системы.	Функциональная модель IDEF0 информационной системы. AS-IS. Функциональная модель IDEF0 информационной системы. TO-BE. Диаграммы поведения Use Case безопасной информационной системы. иаграммы поведения Statechart безопасной информационной системы. Диаграммы поведения Activity безопасной информационной системы. Диаграммы поведения. Collaboration & Sequence.	1	36	Раздел отчета.
2	Анализ защищенности автоматизированной системы.	Классификация информационной системы.	1	36	Раздел отчета.
3	Модели угроз и модели нарушителя информационной	Определение актуальных угроз безопасности информации и разработка на их основе модели угроз.	1	36	Раздел отчета.

	безопасности автоматизированной системы.				
4	Анализ рисков информационной безопасности автоматизированной системы.	Состав мер по защите информации, обеспечивающих блокирование (нейтрализацию) актуальных угроз безопасности информации, и их содержание в соответствии с установленным классом защищенности информационной системы. Расчет информационных рисков.	1	36	Раздел отчета.
5	Разработка мероприятий по снижению информационных рисков.	Определение IT – технологий, требующих снижения информационного риска. Внедрение мер зашиты в информационной системе для снижения рисков. Предварительные испытания системы защиты информации информационной системы. Опытная эксплуатация системы защиты информации информационной системы. Анализ уязвимостей информационной системы.	2	72	Раздел отчета.

8. Научно-исследовательские и научно-производственные технологии, используемые на практике

Научно-исследовательские и научно-производственные технологии, используемые на практике, определяются предприятием.

9. Учебно-методическое обеспечение самостоятельной работы студентов на практике

Контрольные вопросы и задания для проведения аттестации по итогам практики

10. Формы промежуточной аттестации (по итогам практики)

В качестве основной формы отчетности является письменный отчет. Форма контроля прохождения практики - дифференцированный зачет.

По окончании практики студент-практикант составляет письменный отчет и в порядке, установленном кафедрой, сдает его и другие отчетные материалы, предусмотренные методическими указаниями кафедры к прохождению практики, подписанные руководителем практики от организации.

Отчет должен содержать сведения о конкретно выполненной студентом работе в период прохождения практики.

При оценке итогов работы студента принимается во внимание характеристика, данная ему руководителем практики от предприятия.

11. Учебно-методическое и информационное обеспечение практики

а) основная литература:

1. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Приказ ФСТЭК России от 11 февраля 2013 г. N 17.

б) дополнительная литература:

определяется предприятием

в) программное обеспечение и интернет-ресурсы:

определяется предприятием

12. Материально-техническое обеспечение практики

Материально-техническое обеспечение практики определяется предприятием.

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций и ООП ВО по направлению подготовки 10.05.03 «Информационная безопасность автоматизированных систем».

Программу составил: доцент, к.т.н. Федоров Н.В.

Программа утверждена на заседании кафедры «Информационная безопасность» «29» августа 2019 г., протокол № 1.

Заведующий кафедрой

профессор, к. т. н. Н.В. Федоров

Приложение

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
Московский политехнический университет

Направление подготовки:
10.05.03 «Информационная безопасность автоматизированных систем»

ОП (профиль):
«Обеспечение информационной безопасности распределенных информационных систем»
Виды профессиональной деятельности: научно-исследовательская, проектно-конструкторская, контрольно-аналитическая, организационно-управленческая, эксплуатационная.

Кафедра: «Информационная безопасность»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЕ

Состав: 1. Паспорт фонда оценочных средств
2. Оценочные средства для текущей аттестации
3. Оценочные средства для промежуточной аттестации

Составитель:

доцент, к.т.н. Федоров Н.В.

Москва, 2019 год

1. Паспорт фонда оценочных средств

Таблица 1

Научно-исследовательская работа					
ФГОС ВО **10.05.03 «Информационная безопасность автоматизированных систем»**					
КОМПЕТЕНЦИИ		**Перечень компонентов**	**Технология формирования**	**Форма оценочного средства**	**Степени уровней освоения компетенций**
ИНДЕКС	**ФОРМУЛИРОВКА**				
ПК-1	способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке;	**уметь:** - осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке;	самостоятельная работа	Отчет по практике, дифференцированный зачет	Базовый уровень: - уметь осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности; Повышенный уровень: - уметь осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности на иностранном языке;

ПК-2	способностью создавать и исследовать модели автоматизированных систем;	**знать:** - модели автоматизированных систем; **уметь:** проводить анализ защищенности автоматизированных систем **владеть:** -методами создания моделей автоматизированных систем;	самостоятельная работа	Отчет по практике, дифференцированный зачет	Базовый уровень: - уметь модели автоматизированных систем; Повышенный уровень: - уметь создавать и исследовать модели автоматизированных систем;
ПК-3	способностью проводить анализ защищенности автоматизированных систем;	**уметь:** проводить анализ защищенности автоматизированных систем; **владеть:** инструментальными средствами анализа защищенности автоматизированных систем;	самостоятельная работа	Отчет по практике, дифференцированный зачет	Базовый уровень: - уметь проводить анализ защищенности автоматизированных систем; Повышенный уровень: -владеть инструментальными средствами анализа защищенности автоматизированных систем;
ПК-4	способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы;	**уметь:** - разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	самостоятельная работа	Отчет по практике, дифференцированный зачет	Базовый уровень: -уметь разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы

ПК-5	способностью проводить анализ рисков информационной безопасности автоматизированной системы;	**уметь:** - проводить анализ рисков информационной безопасности автоматизированной системы; **владеть:** - методами анализа рисков информационной безопасности автоматизированной системы;	самостоятельная работа	Отчет по практике, дифференцированный зачет	Базовый уровень: - уметь проводить анализ рисков информационной безопасности автоматизированной системы; Повышенный уровень: -владеть различными методами анализа рисков информационной безопасности автоматизированной системы;
ПК-6	способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности;	**уметь:** - проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности;	самостоятельная работа	Отчет по практике, дифференцированный зачет	Базовый уровень: - проводить анализ эффективного применения автоматизированных систем в сфере профессиональной деятельности; Повышенный уровень: проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности;

ПК-7	способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ;	**уметь:** - разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ;	самостоятельная работа	Отчет по практике, дифференцированный зачет	Базовый уровень: - разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ;

1. Оценочные средства для текущей аттестации

Отчет по практике

Отчет о практике должен содержать:

1. Модели автоматизированной системы.
2. Анализ защищенности автоматизированной системы.
3. Модели угроз и модели нарушителя информационной безопасности автоматизированной системы.
4. Анализ рисков информационной безопасности автоматизированной системы.
5. Разработка мероприятий по снижению информационных рисков.

2. Оценочные средства для промежуточной аттестации

Дифференцированный зачет

Вопросы для дифференцированного зачета

1. Функциональная модель IDEF0 информационной системы. AS-IS.
2. Функциональная модель IDEF0 информационной системы. TO-BE.
3. Диаграммы поведения Use Case безопасной информационной системы.
4. Диаграммы поведения Statechart безопасной информационной системы.
5. Диаграммы поведения Activity безопасной информационной системы.
6. Диаграммы поведения. Collaboration & Sequence.
7. Классификация информационной системы.
8. Определение актуальных угроз безопасности информации и разработка на их основе модели угроз.
9. Состав мер по защите информации, обеспечивающих блокирование (нейтрализацию) актуальных угроз безопасности информации, и их содержание в соответствии с установленным классом защищенности информационной системы.
10. Расчет информационных рисков.
11. Определение IT – технологий, требующих снижения информационного риска.
12. Внедрение мер зашиты в информационной системе для снижения рисков.
13. Предварительные испытания системы защиты информации информационной системы.
14. Опытная эксплуатация системы защиты информации информационной системы.
15. Анализ уязвимостей информационной системы.