Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Максимов Алексей Борисович
Должность: директор департамента по образовательной политике
Дата подписания: 13.10.2023 16:56:56
Уникальный программный ключ:
8db180d1a3f02ac9e60521a5672742735c18b1d6

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий

УТВЕРЖДАЮ
Декан факультета
информационных технологий
/Д. Г. Демидов/
«28» апреля 2022 г.

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ
Научно-исследовательская работа

Направление подготовки
10.05.03 «Информационная безопасность автоматизированных систем»

Образовательная программа (профиль подготовки)
«Безопасность открытых информационных систем»

Квалификация выпускника
Специалист по защите информации

Форма обучения
Очная
Год приема - 2022

Москва 2022 г.

Разработчик(и):

Доцент, к.т.н., доцент  /И.В. Калуцкий/

Согласовано:
И.о. заведующего кафедрой «Информационная безопасность».  А.Ю. Гневшев

Руководитель образовательной программы,  А.Ю. Гневшев

Содержание

1 Цели, задачи и планируемые результаты прохождении практики 4
2 Место практики в структуре образовательной программы 7
3 Характеристика практики 7
4 Структура и содержание практики 7
5 Учебно-методическое и информационное обеспечение 8
5.1 Нормативные документы и ГОСТы 8
5.2 Основная литература 8
5.3 Дополнительная литература 8
5.4 Электронные образовательные ресурсы 8
5.5 Лицензионное и свободно распространяемое программное обеспечение 8
5.6 Современные профессиональные базы данных и информационные справочные системы 8
6 Материально-техническое обеспечение 8
7 Методические рекомендации 9
7.1 Методические рекомендации для руководителя по организации практики 9
7.2 Методические указания для обучающихся по освоению дисциплины 9
8 Фонд оценочных средств 9
8.1 Методы контроля и оценивания результатов прохождения практики 9
8.2 Шкала и критерии оценивания результатов прохождения практики 9
8.3 Оценочные средства 9
8.3.1 Текущий контроль 9
8.3.2 Промежуточная аттестация 10

1 Цели, задачи и планируемые результаты прохождении 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.

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.

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

Код и наименование компетенций	Индикаторы достижения компетенции
УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	ИУК-1.1. Анализирует проблемную ситуацию как систему, осуществляет её декомпозицию и определяет связи между ее составляющими. ИУК-1.2. Определяет противоречивость и пробелы в информации, необходимой для решения проблемной ситуации, а также критически оценивает релевантность используемых информационных источников. ИУК-1.3. Разрабатывает и содержательно аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарных подходов с учетом оценки существующих рисков и возможностей их минимизации.
ПК-1 Способность создавать и исследовать модели автоматизированных систем.	ИПК-1.1. Знает: - модели шифров и математические методы их исследования; - основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; - основные характеристики сигналов электросвязи, спектры и виды модуляции; эталонную модель взаимодействия открытых систем; принципы построения и функционирования систем и сетей передачи информации; - требования к шифрам и основные характеристики шифров; модели шифров и математические методы

	их исследования. ИПК-1.2. Умеет: - разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем; - исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений. ИПК-1.3. Владеет: - навыками математического моделирования в криптографии; - методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем; - навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем; - навыками анализа основных характеристик и возможностей телекоммуникационных систем по передаче информации; - навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем.
ПК-2. Способность проводить анализ защищенности автоматизированных систем	ИПК-2.1. Знает: - требования к шифрам и основные характеристики шифров; - модели шифров и математические методы их исследования; - программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях; - технические каналы утечки информации; - возможности технических средств перехвата информации ИПК-2.2. Умеет организовывать защиту информации от утечки по техническим каналам на объектах информатизации ИПК-2.3. Владеет: - навыками организации и обеспечения режима секретности.
ПК-3 Способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	ИПК-3.1. Знает: - основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; - основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические); - основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах. ИПК-3.2.Умеет: - разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем; - анализировать и оценивать угрозы информационной безопасности объекта. ИПК-3.3. Владеет навыками организации и

	обеспечения режима защиты от угроз информационной безопасности объекта.
ПК-4. Способность проводить анализ рисков информационной безопасности автоматизированной системы	ИПК-4.1. Знает: - требования к шифрам и основные характеристики шифров. ИПК-4.2. Умеет: - анализировать и оценивать угрозы информационной безопасности объекта. ИПК-4.3. Владеет методами проведения анализа рисков информационной безопасности объекта
ПК-5. Способность проводить анализ, предлагать и обосновывать выбор решений обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности	ИПК-5.1. Знает: - требования к шифрам и основные характеристики шифров; архитектуру, принципы функционирования, электронную базу современных компьютеров, вычислительных и телекоммуникационных систем; - источники и классификацию угроз информационной безопасности; - основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; - основные информационные технологии, используемые в автоматизированных системах; - основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; - основные комбинаторные и теоретико-графовые алгоритмы, а также способы их эффективной реализации и оценки сложности. ИПК-5.2. Умеет: - анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем; - классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; - проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения. ИПК-5.3. Владеет: - навыками разработки, документирования баз данных с учетом требований по обеспечению информационной безопасности; - методами формирования требований по защите информации; - методиками оценки показателей качества и эффективности ЭВМ и вычислительных систем; - профессиональной терминологией в области информационной безопасности; - навыками анализа основных узлов и устройств современных автоматизированных систем; навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем.
ОПК—8. Способен применять методы научных исследований при проведении разработок в области защиты информации в автоматизированных системах	ИОПК-8.1. Знает методы научных исследований при проведении разработок в области защиты информации в автоматизированных системах; ИОПК-8.2. Умеет применять методы научных исследований при проведении разработок в области

	защиты информации в автоматизированных системах ОПК-8.3 Владеет методами научных исследований при проведении разработок в области защиты информации в автоматизированных системах.

2 Место практики в структуре образовательной программы

Научно-исследовательская работа относится к обязательной части блока Б2.2 «Практики» основной образовательной программы (Б2.2.2).

Данная практика является предшествующей для выполнения выпускной квалификационной работы.

3 Характеристика практики

Тип и вид практики –научно-исследовательская, стационарная.

Способ и форма проведения практики – непрерывно.

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 11 семестре на базе предприятий требуемого профиля.

4 Структура и содержание практики

Общая трудоемкость практики составляет 12 зачетных единицы, 432 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.	2	72	Раздел отчета.
2	Анализ защищенности автоматизированной системы.	Классификация информационной системы.	2	72	Раздел отчета.
3	Модели угроз и модели нарушителя информационной безопасности автоматизированной	Определение актуальных угроз безопасности информации и разработка на их основе модели угроз.	2	72	Раздел отчета.

	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.	2	72	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.	4	144	Раздел отчета.

5 Учебно-методическое и информационное обеспечение

5.1Нормативные документы и ГОСТы

06.032 Специалист по безопасности компьютерных систем и сетей.

06.033 Специалист по защите информации в автоматизированных системах.

5.2Основная литература

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

5.3Дополнительная литература

Определяется предприятием.

5.4Электронные образовательные ресурсы

Определяется предприятием.

5.5Лицензионное и свободно распространяемое программное обеспечение

Определяется предприятием.

5.6Современные профессиональные базы данных и информационные справочные системы

Определяется предприятием.

6 Материально-техническое обеспечение

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».

7 Методические рекомендации

7.1 Методические рекомендации для руководителя по организации практики

Оценка знаний, умений, навыков, характеризующая этапы формирования компетенций, закрепленных за производственной практикой по получению профессиональных умений и профессионального опыта, осуществляется в форме текущего контроля и промежуточной аттестации.

Текущий контроль проводится в течение практики на месте ее проведения руководителем практики от предприятия.

7.2 Методические указания для обучающихся по освоению дисциплины

Контрольные вопросы и задания для проведения аттестации по итогам практики.

8 Фонд оценочных средств

8.1 Методы контроля и оценивания результатов прохождения практики

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

8.2 Шкала и критерии оценивания результатов прохождения практики

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.

8.3 Оценочные средства

8.3.1 Текущий контроль

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.

8.3.2 Промежуточная аттестация

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.