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

преддипломной практики

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 10
2 Место практики в структуре образовательной программы 13
3 Характеристика практики 13
4 Структура и содержание практики 13
5 Учебно-методическое и информационное обеспечение 14
5.1 Нормативные документы и ГОСТы 14
5.2 Основная литература 14
5.3 Дополнительная литература 14
5.4 Электронные образовательные ресурсы 14
6 Материально-техническое обеспечение 14
7 Методические рекомендации 14
8 Фонд оценочных средств 15
8.3.1 Текущий контроль 15
8.3.2 Промежуточная аттестация 16

1 Цели, задачи и планируемые результаты прохождении практики

К **основным задачам** освоения преддипломной практики следует отнести:

- ознакомление с должностными обязанностями сотрудников организации по профилю подготовки;
- освоение способов комплексного применения средств обеспечения информационной безопасности объекта защиты и оценки эффективности принимаемых мер.

К **основным целям** освоения преддипломной практики следует отнести:

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

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
ПК-8. Способность проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	ИПК-8.1. Знает: • требования к шифрам и основные характеристики шифров; • основные информационные технологии, используемые в автоматизированных системах. ИПК-8.2. Умеет: • контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем. ИПК-8.3. Владеет: • навыками участия в экспертизе состояния защищенности информации на объекте защиты; • навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем; • - методами расчета и • инструментального контроля показателей технической защиты информации; • навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности; • методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем; • методами оценки информационных рисков.
ПК-9. Способность участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации	ИПК-9.1. Знает: • требования к шифрам и основные характеристики шифров;

автоматизированных систем	• способы и средства защиты информации от утечки по техническим каналам и контроля эффективности • защиты информации. ИПК-9.2. Умеет проводит экспериментально-исследовательские работы при сертификации средств защиты информации автоматизированных систем, ИПК-9.3. Владеет навыками проведения экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем.
ПК-10. Способность участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации	ИПК-10.1. Знает: • возможности технических средств перехвата информации. ИПК-10.2. Умеет проводить экспериментально-исследовательских работы при аттестации автоматизированных систем с учетом нормативных документов по защите информации. ИПК-10.3 Владеет навыками проведения экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации.
ОПК—13. Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем	ИОПК-13.1. Знает методы и средства диагностики и тестирования систем защиты информации автоматизированных систем; ИОПК-13.2. Умеет проводить анализ уязвимостей систем защиты информации автоматизированных систем. ИОПК-13.3. Владеет способами организации и проведения диагностики и тестирования систем защиты информации автоматизированных систем и проведением анализа уязвимости.
ПК-11. Способность организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности	ИПК-11.1. Знает: • основные понятия и методы в области управленческой деятельности; • порядок выработки и реализации управленческих решений; • содержание управленческой работы руководителя подразделения; • проводить анализ архитектуры и структуры ЭВМ и систем, оценивать эффективность архитектурно-технических решений, реализованных при построении ЭВМ и систем; • содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем. ИПК-11.2. Умеет: • оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения; • осуществлять планирование и организацию работы рабочего коллектива при выполнении поставленных задач; • проводить мониторинг угроз безопасности компьютерных сетей; • контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем; • администрировать подсистемы информационной безопасности

	автоматизированных систем. ИПК-11.3. Владеет: • навыками обоснования, выбора, реализации и контроля результатов управленческого решения; • навыками организации и обеспечения режима секретности; • навыками работы с технической документацией на ЭВМ и вычислительные системы.
ПК-12. Способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы	ИПК-12.1. Знает: • - состав системы управления и требования к ее элементам; • - основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в сетях ЭВМ. ИПК-12.2. Умеет: • - эффективно использовать различные методы и средства защиты информации для компьютерных сетей; ИПК-12.3. Владеет методами проведения выбора программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы.
ОПК—14. Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений	ИОПК-14.1. Знает основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности; 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. ИОПК-14.2. Умеет разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов; исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений; разрабатывать частные политики информационной безопасности информационной безопасности автоматизированных систем. ИОПК-14.3. Владеет методами формирования требований по защите информации; методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем; методами и средствами технической защиты информации.
ПК-13. Способность разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	ИПК-13.1. Знает ГОСТы по оформлению документов по разработке и регламентированию по обеспечению информационной безопасности. ИПК-13.2. Умеет: • разрабатывать, реализовывать, оценивать и

	корректировать процессы менеджмента информационной безопасности; • разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем. ИПК-13.3. Владеет: • навыками, эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, • программных систем с учетом требований по обеспечению информационной безопасности.
ПК-14. Способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	ИПК-14.1. Знает: • основные угрозы безопасности информации и модели нарушителя в автоматизированных системах принципы формирования политики информационной безопасности в автоматизированных системах. ИПК-14.2. Умеет: • эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах; • контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем; • разрабатывать частные политики информационной безопасности информационной безопасности автоматизированных систем. ИПК-14.3. Владеет: • криптографической терминологией; • навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности; • навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем.
ПК-15. Способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	ИПК-15.1. Знает: • основные задачи и понятия криптографии; требования к шифрам и основные характеристики шифров; типовые поточные и блочные шифры. ИПК-15.2. Умеет: • определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем, составлять аналитические обзоры по вопросам обеспечения информационной безопасности автоматизированных систем. ИПК-15.3. Владеет методами формирования комплекса мер по защите информации и ограниченного доступа.

2 Место практики в структуре образовательной программы

Преддипломная практика относится к базовой части блока Б2.2 «Практики» основной образовательной программы (Б2.2.3).

Данная практика является предшествующей для выполнения выпускной квалификационной работы.

3 Характеристика практики

Тип и вид практики – преддипломная, 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 единиц, 432 часа.

№ 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	Структура, история и традиции организации	Структура, история и традиции организации. Нормативные документы, регламентирующие деятельность организации. Основные обязанности должностных лиц организации по профилю подготовки.	1	36	Раздел отчета
2	Основные технологические процессы	Основные технологические процессы и производственное оборудование по профилю деятельности.	2	72	Раздел отчета
3	Стандарты и условия	Действующие стандарты, технические условия, положения и инструкции по эксплуатации аппаратных и программных средств, используемых по профилю деятельности.	2	72	Раздел отчета
4	Технологии защиты информации на предприятии	Функциональные обязанности сотрудника организации по должности, определенной на период практики. Технологии применения программных и аппаратных средств организации для решения профессиональных задач.	4	144	Раздел отчета
5	Методики защиты	Методики применения	3	108	Раздел отчета

	информации	измерительной техники для контроля и изучения отдельных характеристик используемых средств вычислительной техники.				

5 Учебно-методическое и информационное обеспечение

5.1 Нормативные документы и ГОСТы

06.032 Специалист по безопасности компьютерных систем и сетей.

06.033 Специалист по защите информации в автоматизированных системах.

5.2 Основная литература

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

5.3 Дополнительная литература

Определяется предприятием.

5.4 Электронные образовательные ресурсы

Определяется предприятием.

5.5 Лицензионное и свободно распространяемое программное обеспечение

Определяется предприятием.

5.6 Современные 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

1. Структура, история и традиции организации.
2. Нормативные документы, регламентирующие деятельность организации.
3. Основные обязанности должностных лиц организации по профилю подготовки.
4. Основные технологические процессы.
5. Производственное оборудование по профилю деятельности.
6. Действующие стандарты, технические условия, положения и инструкции по эксплуатации аппаратных и программных средств, используемых по профилю деятельности.
7. Функциональные обязанности сотрудника организации по должности, определенной на период практики.
8. Технологии применения программных и аппаратных средств организации для решения профессиональных задач.
9. Методики применения измерительной техники для контроля и изучения отдельных характеристик используемых средств вычислительной техники.

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. Структура, история и традиции организации.
2. Нормативные документы, регламентирующие деятельность организации.

3. Основные обязанности должностных лиц организации по профилю подготовки.
4. Основные технологические процессы.
5. Производственное оборудование по профилю деятельности.
6. Действующие стандарты, технические условия, положения и инструкции по эксплуатации аппаратных и программных средств, используемых по профилю деятельности.
7. Функциональные обязанности сотрудника организации по должности, определенной на период практики.
8. Технологии применения программных и аппаратных средств организации для решения профессиональных задач.
9. Методики применения измерительной техники для контроля и изучения отдельных характеристик используемых средств вычислительной техники.

8.3.2 Промежуточная аттестация

Дифференцированный зачет. Вопросы для дифференцированного зачета

1. Эксплуатационная документация на систему защиты информации автоматизированной системы.
2. Руководство администратора и пользователя средств защиты информации.
3. Состав организационных мер и порядок их реализации.
4. Порядок учета, хранения и использования съемных машинных носителей информации.
5. Порядок вывода информации на внешние носители информации.
6. Правила и порядок генерации, смены и восстановления паролей пользователей, заведения и удаления учетных записей пользователей.
7. Порядок выявления инцидентов, связанных с нарушениями требований о защите информации, и реагирования на эти инциденты.
8. Порядок обслуживания системы защиты информации обслуживающим персоналом.
9. Реализация в соответствии с организационно-распорядительными документами по защите информации правил, регламентирующих права доступа субъектов доступа к объектам доступа (далее - правила разграничения доступа).
10. Введение ограничений на действия пользователей и обслуживающего персонала, а также на изменение условий эксплуатации, состава и конфигурации технических средств обработки информации и программного обеспечения.

11. Проверка полноты и детальности описания в организационно-распорядительных документах по защите информации действий пользователей и администраторов информационной системы по реализации организационных мер.

12. Отработка действий должностных лиц и подразделений, ответственных за реализацию организационных мер.

13. Проверка работоспособности системы защиты информации информационной системы.

14. Принятие решения о возможности опытной эксплуатации системы защиты информации информационной системы.

15. Опытная эксплуатация системы защиты информации информационной системы

16. Проверка функционирования системы защиты информации информационной системы, в том числе реализованных мер по защите информации, а также готовность пользователей и администраторов к эксплуатации системы защиты информации информационной системы.

17. Оценка возможности преодоления нарушителем системы защиты информации информационной системы и предотвращения реализации угроз безопасности информации.

18. Средства контроля (анализа) защищенности информации.

19. Анализ уязвимостей средств защиты информации, технических средств обработки информации и программного обеспечения информационной системы.

20. Правильность установки и настройки средств защиты информации, технических средств обработки информации и программного обеспечения, а также корректность работы средств защиты информации при их взаимодействии с техническими средствами обработки информации и программным обеспечением.

21. Уточнение модели угроз безопасности информации и при необходимости принимаются дополнительные меры по защите информации с целью устранения выявленных уязвимостей.

22. Проверка выполнения требований к системе защиты информации информационной системы в соответствии с техническим заданием на ее создание.