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

УТВЕРЖДЕНО
Декан факультета
Информационных технологий
_____ / А.Ю. Филиппович /
« 28 » мая 2020 г.

РАБОЧАЯ ПРОГРАММА

преддипломной практики

Направление подготовки
10.05.03 «Информационная безопасность автоматизированных систем»

Образовательная программа (профиль подготовки)
«Обеспечение информационной безопасности распределенных информационных систем»

Квалификация выпускника
Специалист по защите информации

Форма обучения
Очная
Год приема - 2020

Москва 2020 г.

1. Цели практики

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.

2. Задачи 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.

3. Место практики в структуре программы

Преддипломная практика относится к базовой части блока 2 «Практики» основной образовательной программы.

Данная практика является предшествующей для выполнения выпускной квалификационной работы.

4. Тип, вид, способ и формы проведения практики

Тип и вид практики – преддипломная, 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 11 семестре на базе предприятий требуемого профиля.

6. Компетенции обучающегося, формируемые в результате прохождения практики

В результате освоения преддипломной 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-8	Способен проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	**уметь:** - проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации; **владеть:** - методами и средствами контрольных проверок работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации;
ПК-9	Способен участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем	**знать:** - процедуру сертификации средств защиты информации; **уметь:** - проводить экспериментально-исследовательские работы при сертификации средств защиты информации;
ПК-10	Способен участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации	**знать:** - процедуру аттестации автоматизированных систем с учетом нормативных документов по защите информации; **уметь:** - проводить экспериментально-исследовательские работы 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	**уметь:** - проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации; **владеть:** - методами и инструментальными средствами мониторинга защищенности информации в автоматизированной системе;
ПК-11	Способен организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности	**уметь:** - организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности;
ПК-12	Способен разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы	**знать:** - систему управления информационной безопасностью автоматизированной системы; **уметь:** - разрабатывать предложения по совершенствованию системы управления информационной безопасностью 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	**уметь:** - организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности;
ПК-13	Способен разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	**знать:** - состав, структуру и содержание документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем; **уметь:** - разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем;
ПК-14	Способен участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	**уметь:** - формировать политику информационной безопасности организации и контролировать эффективность ее реализации;
ПК-15	Способен формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	**уметь:** - формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа;
ПСК-7.5	Способность координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении	**уметь:** координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении

7. 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	Основные технологические	2	72	Раздел отчета

	технологические процессы	процессы и производственное оборудование по профилю деятельности.			
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 информации	Методики применения измерительной техники для контроля и изучения отдельных характеристик используемых средств вычислительной техники.	3	108	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

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.

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» «28» мая 2020 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 ПРЕДДИПЛОМНОЙ ПРАКТИКЕ

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, 2020 год

1. Паспорт фонда оценочных средств

Таблица 1

Преддипломная практика					
ФГОС ВО **10.05.03 «Информационная безопасность автоматизированных систем»**					
КОМПЕТЕНЦИИ		**Перечень компонентов**	**Технология формирования**	**Форма оценочного средства**	**Степени уровней освоения компетенций**
ИНДЕКС	**ФОРМУЛИРОВКА**				
ПК-8	Способен проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	**уметь:** - проводить контрольные проверки работоспособности применяемых программно-ппаратных, криптографических и технических средств защиты информации; **владеть:** - методами и средствами контрольных проверок работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации;	самостоятельная работа	Отчет по практике, дифференцированный зачет	Базовый уровень: -- уметь проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации; Повышенный уровень: - владеть методами и средствами контрольных проверок работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации;

ПК-9	Способен участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем	**знать:** процедуру сертификации средств защиты информации; **уметь:** - проводить экспериментально-исследовательские работы при сертификации средств защиты информации;	самостоятельная работа	Отчет по практике, дифференцированный зачет	Базовый уровень: - знать процедуру сертификации средств защиты информации; Повышенный уровень: - уметь проводить экспериментально-исследовательские работы при сертификации средств защиты информации;
ПК-10	Способен участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации	**знать:** - процедуру аттестации автоматизированных систем с учетом нормативных документов по защите информации; **уметь:** - проводить экспериментально-исследовательские работы при аттестации автоматизированных систем с учетом нормативных документов по защите информации;	самостоятельная работа	Отчет по практике, дифференцированный зачет	Базовый уровень: - знать процедуру аттестации автоматизированных систем с учетом нормативных документов по защите информации; Повышенный уровень: -уметь проводить экспериментально-исследовательские работы 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	**уметь:** - проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации; **владеть:** методами и инструментальными средствами мониторинга защищенности информации в автоматизированной системе;	самостоятельная работа	Отчет по практике, дифференцированный зачет	Базовый уровень: - проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации;
ПК-11	Способен организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности	**уметь:** - организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности;	самостоятельная работа	Отчет по практике, дифференцированный зачет	Базовый уровень: - организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности;

ПК-12	Способен разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы	**знать:** - систему управления информационной безопасностью автоматизированной системы; **уметь:** - разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы;	самостоятельная работа	Отчет по практике, дифференцированный зачет	Базовый уровень: - знать систему управления информационной безопасностью автоматизированной системы; Повышенный уровень: - уметь разрабатывать предложения по совершенствованию системы управления информационной безопасностью 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	**уметь:** - организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности;	самостоятельная работа	Отчет по практике, дифференцированный зачет	Базовый уровень: - уметь организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности;

ПК-13	Способен разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	**знать:** - состав, структуру и содержание документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем; **уметь:** - разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем;	самостоятельная работа	Отчет по практике, дифференцированный зачет	Базовый уровень: - знать состав, структуру и содержание документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем Повышенный уровень: - уметь разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем
ПК-14	Способен участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	**уметь:** - формировать политику информационной безопасности организации и контролировать эффективность ее реализации;	самостоятельная работа	Отчет по практике, дифференцированный зачет	Базовый уровень: - формировать политику информационной безопасности организации и контролировать эффективность ее реализации;
ПК-15	Способен формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	**уметь:** - формировать комплекс мер правила, процедуры, методы) для защиты информации ограниченного доступа;	самостоятельная работа	Отчет по практике, дифференцированный зачет	Базовый уровень: -формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа;

ПСК-7.5	Способность координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении

2. Оценочные средства для текущей аттестации

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.

3. Оценочные средства для промежуточной аттестации

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 так же 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.