

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Максимов Алексей Борисович
Должность: директор департамента по образовательной политике
Дата подписания: 30.10.2023 12:37:09
Уникальный программный ключ:
8db180d1a3f02ac9e60521a5672742735c18b1d6

**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 / А.Ю. Филиппович /
«28» мая 2020 г.

РАБОЧАЯ ПРОГРАММА ПРРАКТИКИ

преддипломной практики

Направление подготовки
10.03.01 «Информационная безопасность»

Образовательная программа (профиль)
«Безопасность компьютерных систем»

Квалификация выпускника
Бакалавр

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;
- формирование представления об информационной безопасности объекта защиты, методах и средствах ее обеспечения;
- 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 блоку 2 «Практики» основной образовательной программы.

Практика базируется на дисциплинах базовой и вариативной части учебного плана.

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 8 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-9	способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	уметь: осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов; составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;
ПК-10	способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	уметь: анализировать и оценивать угрозы информационной безопасности объекта; владеть: методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов;
ПК-11	способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов;	уметь: проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов;
ПК-12	способностью принимать участие в проведении экспериментальных исследований системы защиты информации;	уметь: проводить экспериментальные исследования системы защиты информации;
ПК-13	способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	знать: комплекс мер по обеспечению информационной безопасности на предприятии; уметь: организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности; владеть: методами управления процессом их реализации;
ПК-14	способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности;	уметь: организовывать работу малого коллектива исполнителей в профессиональной деятельности;
ПК-15	способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности	знать: технологический процесс защиты информации ограниченного доступа на предприятии; уметь: организовывать технологический процесс защиты информации ограниченного доступа на предприятии; владеть:

	Российской Федерации, Федеральной службы по техническому и экспортному контролю	навыками безопасного использования технических средств в профессиональной деятельности;
ПСК-1.1	Способность участвовать в разработке формальных моделей политик безопасности, политик управления доступом и информационными потоками в компьютерных системах	уметь: участвовать в разработке формальных моделей политик безопасности, политик управления доступом и информационными потоками в компьютерных системах
ПСК -1.2	Способность использовать математические методы обработки, анализа и синтеза результатов профессиональных исследований	уметь: использовать математические методы обработки, анализа и синтеза результатов профессиональных исследований
ПСК-1.3	Способность выполнять работу по самостоятельному построению алгоритмов, проведению их анализа и реализации в современных программных комплексах	уметь: выполнять работу по самостоятельному построению алгоритмов, проведению их анализа и реализации в современных программных комплексах
ПСК-1.4	Способность проводить экспериментальное исследование компьютерных систем с целью выявления уязвимостей	уметь: проводить экспериментальное исследование компьютерных систем с целью выявления уязвимостей

7. Структура и содержание практики

Общая трудоемкость практики составляет 12 зачетных единиц, 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	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.	3	108	Раздел отчета
4	Технологии защиты информации на предприятии	Функциональные обязанности сотрудника организации по должности, определенной на период практики. Технологии применения программных и аппаратных средств	3	108	Раздел отчета

		организации для решения профессиональных задач.			
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.

10. 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 10.03.01 «Информационная безопасность».

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

Программа утверждена на заседании кафедры «Информационная безопасность» «29» августа 2020 г., протокол № 1.



Заведующий кафедрой
профессор, к. т. н.

Н.В. Федоров

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Направление подготовки: 10.03.01 «Информационная безопасность»

ОП (профиль): «Безопасность компьютерных систем»

Форма обучения: очная

Вид профессиональной деятельности: эксплуатационная; проектно-технологическая;
экспериментально-исследовательская; организационно-управленческая.

Кафедра: «Информационная безопасность»

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
ПО ПРЕДИПЛОМНОЙ ПРАКТИКЕ**

Состав: 1. Паспорт фонда оценочных средств

2. Оценочные средства для текущей аттестации

3. Оценочные средства для промежуточной аттестации

Составители:

проф., к.т.н. Федоров Н.В.

Москва, 2020 год

1. Паспорт фонда оценочных средств

Таблица 1

Преддипломная практика					
ФГОС ВО 10.03.01 «Информационная безопасность»					
КОМПЕТЕНЦИИ		Перечень компонентов	Технология формирования	Форма оценочного средства	Степени уровней освоения компетенций
ИНДЕКС	ФОРМУЛИРОВКА				
ПК-9	<p>способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности</p>	<p>уметь: осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов; составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности</p>	самостоятельная работа	Отчет по практике, дифференцированный зачет	<p style="text-align: center;">Базовый уровень:</p> <p>- подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов;</p> <p style="text-align: center;">Повышенный уровень:</p> <p>- составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;</p>
ПК-10	<p>способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности</p>	<p>уметь: анализировать и оценивать угрозы информационной безопасности объекта;</p> <p>владеть: методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов;</p>	самостоятельная работа	Отчет по практике, дифференцированный зачет	<p style="text-align: center;">Базовый уровень:</p> <p>- анализировать и оценивать угрозы информационной безопасности объекта;</p> <p style="text-align: center;">Повышенный уровень:</p> <p>- проверки защищенности объектов информатизации на соответствие требованиям нормативных документов;</p>

ПК-11	способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов;	уметь: проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов;	самостоятельная работа	Отчет по практике, дифференцированный зачет	<p>Базовый уровень:</p> <p>- проводить эксперименты по заданной методике,</p> <p>Повышенный уровень:</p> <p>- проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов;</p>
ПК-12	способностью принимать участие в проведении экспериментальных исследований системы защиты информации;	уметь: проводить экспериментальные исследования системы защиты информации;	самостоятельная работа	Отчет по практике, дифференцированный зачет	<p>Базовый уровень:</p> <p>- проводить экспериментальные исследования подсистемы защиты информации;</p> <p>Повышенный уровень:</p> <p>- проводить экспериментальные исследования системы защиты информации;</p>
ПК-13	способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	знать: комплекс мер по обеспечению информационной безопасности на предприятии; уметь: организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности; владеть: методами управления процессом их реализации;	самостоятельная работа	Отчет по практике, дифференцированный зачет	<p>Базовый уровень:</p> <p>- поддерживать выполнение комплекса мер по обеспечению информационной безопасности;</p> <p>Повышенный уровень:</p> <p>- организовывать выполнение комплекса мер по обеспечению информационной безопасности;</p>

ПК-14	способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности;	уметь: организовывать работу малого коллектива исполнителей в профессиональной деятельности;	самостоятельная работа	Отчет по практике, дифференцированный зачет	Базовый уровень: - организовывать работу малого коллектива исполнителей в профессиональной деятельности; Повышенный уровень: - создавать и организовывать работу малого коллектива исполнителей в профессиональной деятельности;
ПК-15	способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	знать: технологический процесс защиты информации ограниченного доступа на предприятии; уметь: организовывать технологический процесс защиты информации ограниченного доступа на предприятии; владеть: навыками безопасного использования технических средств в профессиональной деятельности;	самостоятельная работа	Отчет по практике, дифференцированный зачет	Базовый уровень: - поддерживать технологический процесс защиты информации ограниченного доступа на предприятии; Повышенный уровень: - организовывать технологический процесс защиты информации ограниченного доступа на предприятии;
ПСК-1.1	Способность участвовать в разработке формальных моделей политик безопасности, политик управления доступом и информационными потоками в компьютерных системах	уметь: участвовать в разработке формальных моделей политик безопасности, политик управления доступом и информационными потоками в компьютерных системах	самостоятельная работа	Отчет по практике, дифференцированный зачет	Базовый уровень: уметь: участвовать в разработке формальных моделей политик безопасности, политик управления доступом и информационными потоками в компьютерных системах

ПСК-1.2	Способность использовать математические методы обработки, анализа и синтеза результатов профессиональных исследований	уметь: использовать математические методы обработки, анализа и синтеза результатов профессиональных исследований	самостоятельная работа	Отчет по практике, дифференцированный зачет	Базовый уровень: уметь: использовать математические методы обработки, анализа и синтеза результатов профессиональных исследований
ПСК-1.3	Способность выполнять работу по самостоятельному построению алгоритмов, проведению их анализа и реализации в современных программных комплексах	уметь: выполнять работу по самостоятельному построению алгоритмов, проведению их анализа и реализации в современных программных комплексах	самостоятельная работа	Отчет по практике, дифференцированный зачет	Базовый уровень: уметь: выполнять работу по самостоятельному построению алгоритмов, проведению их анализа и реализации в современных программных комплексах
ПСК-1.4	Способность проводить экспериментальное исследование компьютерных систем с целью выявления уязвимостей	уметь: проводить экспериментальное исследование компьютерных систем с целью выявления уязвимостей	самостоятельная работа	Отчет по практике, дифференцированный зачет	Базовый уровень: уметь: проводить экспериментальное исследование компьютерных систем с целью выявления уязвимостей

2. Оценочные средства для текущей аттестации

Отчет по практике

Отчет о практике должен содержать:

1. Структура, история и традиции организации.
2. Основные технологические процессы.
3. Стандарты и условия.
4. Технологии защиты информации на предприятии.
5. Методики защиты информации.

3. Оценочные средства для промежуточной аттестации

Дифференцированный зачет

Вопросы для дифференцированного зачета

10. Структура, история и традиции организации.
11. Нормативные документы, регламентирующие деятельность организации.
12. Основные обязанности должностных лиц организации по профилю подготовки.
13. Основные технологические процессы.
14. Производственное оборудование по профилю деятельности.
15. Действующие стандарты, технические условия, положения и инструкции по эксплуатации аппаратных и программных средств, используемых по профилю деятельности.
16. Функциональные обязанности сотрудника организации по должности, определенной на период практики.
17. Технологии применения программных и аппаратных средств организации для решения профессиональных задач.
18. Методики применения измерительной техники для контроля и изучения отдельных характеристик используемых средств вычислительной техники.