ГАОУ ВО «Дагестанский государственный университет народного хозяйства»

Факультет «Информационные технологии и управление»

Основная профессиональная образовательная программа высшего образования

- программа бакалавриата по направлению подготовки

10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем»

АННОТАЦИИ РАБОЧИХ ПРОГРАММ ПРАКТИК

Махачкала - 2020

Учебная практика (практика по получению первичных профессиональных умений и навыков)

Цель прохождения практики

Целью учебной практики является закрепление и расширение теоретических и практических знаний, полученных за время обучения; изучение литературы и нормативно-методической документации по профилю подготовки; приобретение заданных компетенций для будущей профессиональной деятельности; приобретение первоначальных практических навыков выполнения работ по обслуживанию технических средств защиты информации.

Вид практики, способ и формы ее проведения

Вид практики – учебная практика.

Тип практики - практика по получению первичных профессиональных умений и навыков.

Способ проведения учебной практики – стационарная.

Форма проведения практики – дискретная, путем выделения непрерывного периода учебного времени для проведения практики.

Место проведения практики - учебная практика проводится в компьютерных и мультимедийных аудиториях факультета «Информационные технологии и управление» ГАОУ ВО ДГУНХ.

Компетенции выпускников, формируемые в результате прохождения практики

код компетенции	формулировка компетенции
ОК	**ОБЩЕКУЛЬТУРНЫЕ КОМПЕТЕНЦИИ**
ОК-5	Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики.
ОК-8	Способность к самоорганизации и самообразованию.
ОПК	**ОБЩЕПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ**
ОПК-2	Способность применять соответствующий математический аппарат для решения профессиональных задач
ПК	**ПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ**
ПК-1	Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации.
ПК-2	Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач.
ПК-3	Способность администрировать подсистемы информационной безопасности объекта защиты.
ПК-11	Способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов

ПСК	**ПРОФЕССИОНАЛЬНО-СПЕЦИАЛИЗИРОВАННЫЕ КОМПЕТЕНЦИИ**
ПСК-1	Способность учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации
ПСК-2	Способность выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей
ПСК-3	Способность планировать и организовывать комплекс мероприятий по защите информации, связанных с обеспечением надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации
ПСК-4	Способность участвовать в разработке аппаратных и программных средств в составе автоматизированных систем, связанных с обеспечением информационной безопасности

Планируемые результаты обучения по практике

Формируемые компетенции	***Планируемые результаты обучения при прохождении практики***	
	Умения	***Навыки или практический опыт деятельности***
ОК-5	соблюдать нормы профессиональной этики	владения профессиональной терминологией в области информационной безопасности
ОК-8	системно анализировать, обобщать информацию, формулировать цели и самостоятельно находить пути их достижения	самостоятельной работы при решении задач защиты информации
ОПК-2	использовать математические методы и модели для решения прикладных задач.	компьютерной реализации криптографических алгоритмов
ПК-1	устанавливать и настраивать программные и аппаратные средства защиты информации	установки и настройки специализированного программного обеспечения.
ПК-2.	применять программные средства системного, прикладного и специального назначения	безопасного использования технических средств в профессиональной деятельности
ПК-3.	администрировать подсистемы информационной безопасности вычислительных сетей	управления информационной безопасностью информационных систем и сетей
ПК-11.	формулировать цели и задачи исследования	планирования эксперимента
ПСК-1.	учитывать и использовать особенности архитектуры сетей передачи информации для организации защиты обрабатываемой информации	конфигурирования параметров системы защиты информации
ПСК-2.	администрировать подсистему информационной безопасности компьютерной сети	конфигурирования параметров системы защиты информации

ПСК-3.	планировать и организовывать работу по обеспечению защиты информации в компьютерных сетях; организовывать защиту обрабатываемой информации криптографическими методами	реализации криптографических методов защиты информации
ПСК-4.	разрабатывать программные и аппаратные средства обеспечения информационной безопасности.	проектирования и реализации программных средств для обеспечения информационной безопасности

Место практики в структуре ОПОП

Учебная практика (практика по получению первичных профессиональных умений и навыков) является составной частью ОПОП ВО – программы бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профилю «Безопасность автоматизированных систем» и в полном объеме относится к вариативной части этой программы.

Учебная практика является обязательным этапом обучения бакалавра по направлению подготовки 10.03.01 Информационная безопасность, профилю «Безопасность автоматизированных систем» и предусматривается учебным планом в Блоке 2 «Практики».

Практика проводится в 5 и 6 семестрах по 1 неделе.

Практика организуется после изучения дисциплин «Информатика», «Языки программирования», «Технологии и методы программирования», «Основы информационной безопасности», «Теория информации», «Организационно-правовое обеспечение информационной безопасности», «Криптографические методы защиты информации».

Трудоемкость практики

Общая трудоемкость учебной практики составляет 3 зачетные единицы.

Продолжительность практики составляет 2 недели.

Результаты прохождения практики оцениваются посредством проведения промежуточной аттестации в виде защиты отчета по практике.

Прохождение практики осуществляется в два периода:

- 1 неделя реализуется в 5 семестре, после окончания теоретического обучения;
- 2 неделя реализуется в 6 семестре, после окончания теоретического обучения.

Сроки практики для обучающихся определяются учебным планом и календарным учебным графиком по направлению подготовки 10.03.01 Информационная безопасность, профилю «Безопасность автоматизированных систем».

Содержание практики

Подготовительный этап

- знакомство практиканта с программой прохождения практики;
- инструктаж по технике безопасности и особенностями работы с программно-аппаратными комплексами защиты информации

Ознакомительный этап

- Обзор основных стандартов и требований криптографической защиты информации
- Российский стандарт шифрования ГОСТ 28147-89
- Алгоритм DES
- Система обмена ключами Диффи-Хеллмана
- Шифр RSA
- Шифр Эль-Гамаля
- Метода факторизации целых чисел - «Шаг младенца, шаг великана»
- Генерация и проверка подписей RSA
- Генерация и проверка подписей по ГОСТ Р34.10-94
- Установка и настройка программного обеспечения «ViPNet Administrator»
- Работа с технологиями ЦУС и УКЦ
- Работа с мастером-ключей, DST-файлами. Работа с ключами для связи АП с ЦУСом и сервером
- Построение сетевой и прикладной структуры ViPNet-сети
- Модификация с использованием и без использования компрометации
- Модификация межсетевого взаимодействия защищенных сетей ViPNet

Заключительный этап

Аннотация рабочей программы учебной практики (практики по получению первичных профессиональных умений и навыков) разработана к.п.н., доцентом кафедры «Информационные технологии и информационная безопасность» Гасановой З.А.

Производственная практика (эксплуатационная практика)

Цель прохождения практики

Цель производственной практики (эксплуатационной практики) – закрепление и углубление теоретических знаний по информационной безопасности и защите информации, программно-техническим, организационным и правовым методам обеспечения информационной безопасности, приобретение практических профессиональных навыков и компетенций, опыта самостоятельной профессиональной деятельности.

Вид практики, способ и формы ее проведения

Вид практики – производственная практика.

Тип практики - эксплуатационная практика.

Способы проведения практики – стационарная и выездная.

Форма проведения практики – дискретная, путем выделения непрерывного периода учебного времени для проведения практики.

Место проведения практики.

Практика проводится в организациях или на предприятиях любых организационно-правовых форм, с которыми у ГАОУ ВО «Дагестанский государственный университет народного хозяйства» заключен договор об организации проведения практики обучающихся, а также в структурных подразделениях ГАОУ ВО «Дагестанский государственный университет народного хозяйства».

Компетенции выпускников, формируемые в результате прохождения практики

код компетенции	формулировка компетенции
ОК	**ОБЩЕКУЛЬТУРНЫЕ КОМПЕТЕНЦИИ**
ОК-5	Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики.
ОК-6	Способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия.
ОК-7	Способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности.
ОК-8	Способность к самоорганизации и самообразованию.
ПК	**ПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ**
ПК-1	Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации.
ПК-2	Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач.

ПК-3	Способность администрировать подсистемы информационной безопасности объекта защиты.
ПК-4	Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты.
ПК-5	Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации
ПК-6	Способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации
ПК-9	Способность 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	Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности.
ПК-14	Способность организовать работу малого коллектива исполнителей в профессиональной деятельности
ПК-15	Способность организовать 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
ПСК	**ПРОФЕССИОНАЛЬНО-СПЕЦИАЛИЗИРОВАННЫЕ КОМПЕТЕНЦИИ**
ПСК-1	Способность учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации
ПСК-2	Способность выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей

Планируемые результаты обучения по практике

Формируемые компетенции	***Планируемые результаты обучения при прохождении практики***	
	Умения	***Навыки или практический опыт деятельности***
ОК-5: Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	соблюдать нормы профессиональной этики	владения профессиональной терминологией в области информационной безопасности

ОК-6: Способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия.	формулировать индивидуальные, групповые и организационные цели; оценивать эффективность управленческих решений в области защиты информации;	работы в коллективе, в том числе в качестве лидера
ОК-7: Способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности	читать и переводить научно- техническую литературу на иностранном языке по профессиональной тематике, правильно употреблять терминологическую лексику в профессиональной речи	создания на русском языке грамотных и логически непротиворечивых письменных и устных текстов учебной и научной тематики реферативного характера
ОК-8: Способность к самоорганизации и самообразованию	приобретать новые знания и умения; системно анализировать, обобщать информацию, формулировать цели и самостоятельно находить пути их достижения при решении профессиональных задач;	приобретения новых знаний и умений.
ПК-1. Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации.	Устанавливать и настраивать программные и аппаратные средства защиты информации	установки и настройки специализированного программного обеспечения.
ПК-2. Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач.	применять программные средства системного, прикладного и специального назначения	безопасного использования технических средств в профессиональной деятельности
ПК-3. Способность администрировать подсистемы информационной безопасности объекта защиты.	администрировать подсистемы информационной безопасности вычислительных сетей	управления информационной безопасностью информационных систем и сетей
ПК-4. Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты.	определять комплекс мер (правила, процедуры, практи-ческие приемы, руководящие принципы, методы, средства) для обеспечения	проверки защи-щенности объектов информатизации на соответствие требованиям нормативных документов.

	информационной безопасности информационных систем.	
ПК-5. Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	осуществлять правовую оценку объекта информатизации; проводить аттестацию объекта информатизации по требованиям безопасности информации	осуществления правовой оценки объекта; способами проведения анализа информационной безопасности объекта
ПК-6. Способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	использовать методику контрольных проверок работоспособности и эффективности программных и программно-аппаратных средств защиты информации	анализа работоспособности и эффективности программных и программно-аппаратных средств защиты информации
ПК-9. Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности.	применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем.	поиска нормативной правовой информации по вопросам обеспечения информационной безопасности
ПК-10. Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности.	проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности.	проведения регламентных и проверочных работ по проверке соблюдения требований стандартов в области информационной безопасности
ПК-14. Способность организовать работу малого коллектива исполнителей в профессиональной деятельности	организовать работу в группе по обеспечению информационной безопасности информационной системы, настройке и тестированию программно-аппаратных и технических средств; анализировать предложения участников группы по улучшению	распределения ролей участников группы

	информационной защиты организации	
ПК-15. Способность организовать 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	применять нормативные правовые акты и нормативные методические документы ФСБ России и ФСТЭК России	работы с методические документы регуляторов
ПСК-1. Способность учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации	разрабатывать технические меры защиты информации, с учетом особенностей применяемые информационных технологий	анализа и документирования технических характеристик автоматизированных систем, используемых в организации
ПСК-2. Способность выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей	определять подлежащие защите информационные ресурсы автоматизированных систем; разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем.	конфигурирования параметров системы защиты информации автоматизированных систем.

Место практики в структуре ОПОП

Производственная практика является составной частью ОПОП ВО – программы бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профилю «Безопасность автоматизированных систем» и в полном объеме относится к вариативной части этой программы.

Производственная практика является обязательным этапом обучения бакалавра по направлению подготовки 10.03.01 Информационная безопасность, профилю «Безопасность автоматизированных систем» и предусматривается учебным планом в Блоке 2 «Практики».

Производственная практика является важнейшим элементом учебного процесса на заключительном этапе обучения. Она обеспечивает закрепление и расширение знаний, полученных при изучении теоретических дисциплин, овладение навыками практической работы, приобретение опыта работы в трудовом коллективе.

Трудоемкость практики

Общая трудоемкость производственной практики составляет 9 зачетных единиц (324 академических часа).

Продолжительность практики составляет 6 недель.

Результаты прохождения практики оцениваются посредством проведения промежуточной аттестации в виде защиты отчета по практике.

Сроки практики для обучающихся определяются учебным планом и календарным учебным графиком по направлению подготовки 10.03.01 Информационная безопасность, профилю «Безопасность автоматизированных систем».

При реализации производственной практики образовательная деятельность организована в форме практической подготовки.

Содержание практики

Подготовительный этап: Общие сведения об организации - базе практики.

- Инструктаж по технике безопасности, правилам внутреннего распорядка организации и правилам охраны труда
- Обсуждение совместного рабочего графика (плана) проведения практики с руководителем практики от производства, порядок его реализации
- Изучение технологии работы объекта практики
- Анализ нормативных и правовых актов предприятия/организации
- Анализ информационных средств и компьютерных программ, применяемых на предприятии/организации

Основной этап: Эксплуатация средств защиты информации

- Обзор средств защиты информации установленных на объекте практики
- Изучение технической документации на устройства защиты информации
- Работа с нормативными и правовыми документами
- Организация работы коллектива по организации информационной безопасности на предприятии
- Эксплуатация программных, программно-аппаратных и технических средств прикладного и системного назначения
- Установка, конфигурирование и обслуживание средств защиты информации
- Администрирование подсистемы информационной безопасности на объекте защиты
- Сопровождение и аттестация объекта информатизации на соответствии требованиям по защите информации
- Эксплуатация подсистем управления информационной безопасности
- Мониторинг работоспособности и анализ эффективности реализованных мер защиты информации на объекте практики
- Выполнение индивидуального задания

Заключительный этап: Промежуточная аттестация

- Систематизация материала, подготовка отчета

Аннотация рабочей программы производственной практики (эксплуатационной практики) разработана к.п.н., доцентом кафедры «Информационные технологии и информационная безопасность» Гасановой З.А.

Преддипломная практика

Цель прохождения практики

Целью преддипломной практики является приобретение учащимися практических навыков и компетенций в сфере профессиональной деятельности и подготовка выпускной квалификационной работы.

Вид практики, способ и формы ее проведения

Вид практики – производственная практика.

Тип практики – преддипломная практика.

Способы проведения практики – стационарная и выездная.

Форма проведения практики – дискретная, путем выделения непрерывного периода учебного времени для проведения практики.

Место проведения практики.

Практика проводится в организациях или на предприятиях любых организационно-правовых форм, с которыми у ГАОУ ВО «Дагестанский государственный университет народного хозяйства» заключен договор об организации проведения практики обучающихся, а также в структурных подразделениях ГАОУ ВО «Дагестанский государственный университет народного хозяйства».

Компетенции выпускников, формируемые в результате прохождения практики

код компетенции	формулировка компетенции
ОК	**ОБЩЕКУЛЬТУРНЫЕ КОМПЕТЕНЦИИ**
ОК-5	Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики.
ОК-6	Способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия.
ОК-7	Способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности.
ОК-8	Способность к самоорганизации и самообразованию.
ОПК	**ОБЩЕПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ**
ОПК-5	Способность использовать нормативные правовые акты в профессиональной деятельности
ОПК-7	Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты
ПК	**ПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ**

ПК-1	Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации.
ПК-2	Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач.
ПК-3	Способность администрировать подсистемы информационной безопасности объекта защиты.
ПК-4	Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты.
ПК-5	Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации
ПК-6	Способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации
ПК-7	Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений
ПК-8	Способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов
ПК-9	Способность 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	Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности.
ПК-11	Способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов
ПК-12	Способность принимать участие в проведении экспериментальных исследований системы защиты информации
ПК-13	Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации
ПК-14	Способность организовать работу малого коллектива исполнителей в профессиональной деятельности
ПК-15	Способность организовать 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
ПСК	**ПРОФЕССИОНАЛЬНЫЕ СПЕЦИАЛЬНЫЕ КОМПЕТЕНЦИИ**
ПСК-1	Способность учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации
ПСК-2	Способность выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей

ПСК-3	Способность планировать и организовывать комплекс мероприятий по защите информации, связанных с обеспечением надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации
ПСК-4	Способность участвовать в разработке аппаратных и программных средств в составе автоматизированных систем, связанных с обеспечением информационной безопасности

Планируемые результаты обучения по практике

Формируемые компетенции	***Планируемые результаты обучения при прохождении практики***	
	Умения	***Навыки или практический опыт деятельности***
ОК-5: Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	соблюдать нормы профессиональной этики	владения профессиональной терминологией в области информационной безопасности
ОК-6: Способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия.	формулировать индивидуальные, групповые и организационные цели; оценивать эффективность управленческих решений в области защиты информации;	работы в коллективе, в том числе в качестве лидера
ОК-7: Способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности	читать и переводить научно- техническую литературу на иностранном языке по профессиональной тематике, правильно употреблять терминологическую лексику в профессиональной речи	создания на русском языке грамотных и логически непротиворечивых письменных и устных текстов учебной и научной тематики реферативного характера
ОК-8: Способность к самоорганизации и самообразованию	приобретать новые знания и умения; системно анализировать, обобщать информацию, формулировать цели и самостоятельно находить пути их достижения при решении профессиональных задач;	приобретения новых знаний и умений.
ОПК-5. Способность использовать нормативные правовые акты в профессиональной деятельности	применять правовые акты в профессиональной деятельности	работы с нормативными и методическими документами

ОПК-7. Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	определять информационные ресурсы, подлежащие защите, угрозы безопасности информации	классификации информации ограниченного доступа
ПК-1. Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации.	устанавливать технические средства защиты информации; грамотно эксплуатировать средства в соответствии с их технико-эксплуатационной документацией	конфигурации средств защиты в соответствии с требованиями документов по обеспечению информационной безопасности на предприятии
ПК-2. Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач.	использовать программные и аппаратные средства персонального компьютера	правилами использования программных и аппаратных средств персонального компьютера
ПК-3. Способность администрировать подсистемы информационной безопасности объекта защиты.	производить модернизацию подсистем безопасности объекта защиты в соответствии с руководящими документами	администрирования подсистем безопасности объекта защиты
ПК-4. Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты.	формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе	реализации политики безопасности на объекте практики
ПК-5. Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	осуществлять правовую оценку объекта информатизации; применять нормативные правовые акты и нормативные методические документы в области информационной безопасности; производить анализ информационной безопасности объекта	применения правовых актов и нормативных методических документов в области информационной безопасности
ПК-6. Способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности	использовать методику контрольных проверок работоспособности и эффективности	анализа работоспособности и эффективности программных и

применяемых программных, программно-аппаратных и технических средств защиты информации	программных и программно-аппаратных средств защиты информации	программно-аппаратных средств защиты информации
ПК-7. Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	анализа исходных данных при проектировании подсистем и средств обеспечения информационной безопасности
ПК-8. Способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	оформлять рабочую документацию с учетом действующих нормативных и методических документов	оформления рабочей документации с учетом действующих нормативных и методических документов
ПК-9. Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности.	грамотно применять правовые документы для организации информационной безопасности на предприятии	проведения и обобщения результатов анализа информации, полеченной из различных официальных документов и научной литературы
ПК-10. Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности.	определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; разрабатывать модели угроз и нарушителей информационной безопасности информационных систем	мониторинга и аудита, выявления угроз информационной безопасности информационных систем
ПК-11. Способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	проводить эксперименты по заданной методике, обработку результатов	проведения экспериментов и обработки результатов
ПК-12. Способность принимать участие в проведении экспериментальных исследований системы защиты информации	принимать участие в проведении экспериментальных исследований системы защиты информации	проведения обследования объекта защиты информации на основании эксперимента
ПК-13. Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности	организации мер по обеспечению информационной безопасности

ПК-14. Способность организовать работу малого коллектива исполнителей в профессиональной деятельности	организовать работу в группе по обеспечению информационной безопасности информационной системы	применения профессиональной терминологии по информационной безопасности
ПК-15. Способность организовать 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	разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации.	работы с нормативными правовыми актами
ПСК-1. Способность учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации	разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем.	конфигурирования параметров системы защиты информации автоматизированных систем.
ПСК-2. Способность выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей	администрировать подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей	конфигурирования параметров системы защиты информации автоматизированных систем.
ПСК-3. Способность планировать и организовывать комплекс мероприятий по защите информации, связанных с обеспечением надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации	анализировать программные и программно-аппаратные решения при проектировании системы защиты информации с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах	подготовки документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации
ПСК-4. Способность участвовать в разработке аппаратных и программных средств в составе автоматизированных систем, связанных с обеспечением информационной безопасности	разрабатывать программные и аппаратные средства обеспечения информационной безопасности.	проектирования и реализации программных средств для обеспечения информационной безопасности

Место практики в структуре ОПОП

Преддипломная практика является составной частью ОПОП ВО – программы бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профилю «Безопасность автоматизированных систем» и в полном объеме относится к вариативной части этой программы.

Преддипломная практика является обязательным этапом обучения бакалавра по направлению подготовки 10.03.01 Информационная безопасность, профилю «Безопасность автоматизированных систем» и предусматривается учебным планом в Блоке 2 «Практики».

Преддипломная практика является важнейшим элементом учебного процесса на заключительном этапе обучения. Она обеспечивает закрепление и расширение знаний, полученных при изучении теоретических дисциплин, овладение навыками практической работы, приобретение опыта работы в трудовом коллективе, выполнение выпускной квалификационной работы.

Трудоемкость практики

Общая трудоемкость преддипломной практики составляет 6 зачетных единиц.

Продолжительность практики составляет 4 недели.

Результаты прохождения практики оцениваются посредством проведения промежуточной аттестации в виде защиты отчета по практике.

Сроки практики для обучающихся определяются учебным планом и календарным учебным графиком по направлению подготовки 10.03.01 Информационная безопасность, профилю «Безопасность автоматизированных систем».

При реализации производственной практики образовательная деятельность организована в форме практической подготовки

Содержание практики

Подготовительный этап: Общие сведения об организации - базе практики

- Инструктаж по технике безопасности, правилам внутреннего распорядка организации и правилам охраны труда
- Обсуждение совместного рабочего графика (плана) проведения практики с руководителем практики от производства, порядок его реализации
- Изучение технологии работы объекта практики
- Анализ нормативных и правовых актов предприятия/организации
- Анализ информационных средств и компьютерных программ, применяемых на предприятии/организации

Основной этап: Сбор материала для выполнения выпускной квалификационной работы

- Анализ исходных данных для проектирования системы информационной безопасности на объекте практики
- Мониторинг работоспособности и анализ эффективности мер, реализуемых на объекте практики
- Работа с технической литературой и нормативными и правовыми документами
- Формирование комплекса мер по обеспечению информационной безопасности на объекте практики
- Разработка подсистем управления информационной безопасностью

- Оформление рабочей документации с учетом действующих нормативной и технической документации
- Формирование требований политики безопасности на объекте практики и ее реализация
- Выполнение индивидуального задания

Заключительный этап: Промежуточная аттестация

- Систематизация материала, подготовка отчета

Аннотация рабочей программы преддипломной практики разработана к.п.н., доцентом кафедры «Информационные технологии и информационная безопасность» Гасановой З.А.