ГАОУ ВО «Дагестанский государственный университет народного хозяйства»

Факультет информационных технологий и инженерии

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 - 2023

Учебная практика (учебно-лабораторная практика)

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 – учебно-лабораторная практика.

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 информационных технологий и инженерии ГАОУ ВО ДГУНХ.

Компетенции выпускников, формируемые в результате прохождения практики

код компетенции	формулировка компетенции
ОПК	**ОБЩЕПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ**
ОПК-7.	Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности
ОПК-9.	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности
ОПК-10.	Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты
ОПК-4.2.	Способен администрировать операционные системы, системы управления базами данных, вычислительные сети
ОПК-4.3.	Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем

Планируемые результаты обучения по практике

Код и наименование компетенции	*Код и наименование индикатора достижения компетенции*	*Планируемые результаты обучения при прохождении практики*	
		Умения	*Навыки или практический опыт деятельности*
ОПК-7. Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности	ИОПК-7.3. Разрабатывает и реализовывает на языке высокого уровня алгоритмы решения профессиональных задач	использовать математические методы и модели для решения прикладных задач.	компьютерной реализации криптографических алгоритмов
ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ИОПК-9.1. Использует типовые криптографические средства защиты информации, в том числе средства электронной подписи	использовать типовые криптографические алгоритмы и средства защиты информации	применения средств криптографической защиты информации
ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ИОПК-10.2. Подбирает и конфигурирует программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности	подбирать и настраивать криптографические средства защиты информации в соответствии с заданными политиками безопасности	конфигурирования криптографических средства защиты информации в соответствии с заданными политиками безопасности
ОПК-4.2. Способен администрировать операционные системы, системы управления базами данных, вычислительные сети	ИОПК-4.2.3. Проектирует и настраивает вычислительные сети	администрировать подсистему информационной безопасности компьютерной сети	проектирования системы информационной безопасности компьютерной сети
ОПК-4.3. Способен выполнять работы по установке, настройке, администрированию, обслуживанию и	ИОПК-4.3.1. Применяет программные, программно-аппаратные (в том числе	применять программные и программно-аппаратные средства защиты информации	администрирования программных, программно-аппаратных (в том числе криптографических)

проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем	криптографические) средства защиты информации автоматизированных систем	автоматизированных систем	средств защиты информации автоматизированных систем
	ИОПК-4.3.2. Выполняет установку, настройку и обслуживание технических средств защиты информации автоматизированных систем	устанавливать и настраивать технические средства защиты информации автоматизированных систем	настройки технических средств защиты информации автоматизированных систем

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», «Методы и средства криптографической 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
ПК	**ПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ**
ПК-1	Способен выполнять комплекс задач администрирования подсистем информационной безопасности и управления информационной безопасностью операционных систем, систем управления базами данных и компьютерных сетей
ПК-2	Способен учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации

Планируемые результаты обучения по практике

Код и наименование компетенции	***Код и наименование индикатора достижения компетенции***	***Планируемые результаты обучения при прохождении практики***	
		Умения	***Навыки или практический***

			опыт деятельности
ПК-1. Способен выполнять комплекс задач администрирования подсистем информационной безопасности и управления информационной безопасностью операционных систем, систем управления базами данных и компьютерных сетей	ИПК-1.1 Администрирует подсистему защиты информации операционных систем	планировать политику безопасности операционных систем	управления информационной безопасностью операционных систем
	ИПК-1.2. Администрирует подсистему защиты информации СУБД	планировать политику безопасности СУБД	управления информационной безопасностью СУБД
	ИПК-1.3. Администрирует подсистему защиты информации компьютерных сетей	планировать политику безопасности вычислительных сетей	управления информационной безопасностью вычислительных сетей
	ИПК-1.4. Использует криптографическое методы защиты информации в автоматизированных системах	использовать криптографические методы и средства защиты информации в автоматизированных системах	применения средств криптографической защиты информации в автоматизированных системах
	ИПК-1.5. Управляет защитой информации в автоматизированных системах	классифицировать и оценивать угрозы безопасности информации; Определять подлежащие защите информационные ресурсы автоматизированных систем; конфигурировать параметры системы защиты информации автоматизированных систем	составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе; Устранения неисправностей в работе системы защиты информации автоматизированной системы

ПК-2. Способен учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации	ИПК-2.1. Устанавливает и налаживает средства защиты информации в автоматизированных системах	администрировать программные средства системы защиты информации автоматизированных систем	установки и настройки технических и программных средств системы защиты информации автоматизированной системы
	ИПК-2.2. Обеспечивает безопасность информационных технологий, применяемых в автоматизированных системах	классифицировать и оценивать угрозы безопасности информации автоматизированной системы; разрабатывать предложения по совершенствованию системы управления защитой информации автоматизированной системы	проведения анализа уязвимостей автоматизированных и информационных 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 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: 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
УК	**УНИВЕРСАЛЬНЫЕ КОМПЕТЕНЦИИ**
УК-6	Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни
ПК	**ПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ**
ПК-1	Способен выполнять комплекс задач администрирования подсистем информационной безопасности и управления информационной безопасностью операционных систем, систем управления базами данных и компьютерных сетей
ПК-2	Способен учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации
ПК-3	Способен учитывать и использовать особенности средств защиты информации при формировании системы защиты информации автоматизированных систем
ПК-4	Способен планировать и организовывать комплекс мероприятий и разрабатывать организационно-распорядительную документацию по защите информации

Планируемые результаты обучения по практике

Код и наименование компетенции	*Код и наименование индикатора достижения компетенции*	*Планируемые результаты обучения при прохождении практики*	
		Умения	***Навыки или практический опыт деятельности***
УК-6. Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни	ИУК-6.1. Использует инструменты и методы управления временем при выполнении конкретных задач, проектов, при достижении поставленных целей	использовать инструменты и методы управления временем при выполнении задач преддипломной практики	применения инструментов и методов управления временем
	ИУК-6.2. Определяет приоритеты собственной деятельности, личностного развития и профессионального роста, строит профессиональную карьеру и определяет стратегию профессионального развития	определять приоритеты собственной деятельности	определения приоритетов собственной деятельности
	ИУК-6.3. Оценивает эффективность использования времени и ресурсов при решении поставленных целей и задач	оценивать эффективность использования времени и ресурсов при решении поставленных целей и задач	
ПК-1. Способен выполнять комплекс задач администриро	ИПК-1.1 Администрирует подсистему защиты информации операционных систем	планировать политику безопасности операционных систем	управления информационной безопасностью операционных систем

вания подсистем информационной безопасности и управления информационной безопасностью операционных систем, систем управления базами данных и компьютерных сетей	ИПК-1.2. Администрирует подсистему защиты информации СУБД	планировать политику безопасности СУБД	управления информационной безопасностью СУБД
	ИПК-1.3. Администрирует подсистему защиты информации компьютерных сетей	планировать политику безопасности вычислительных сетей	управления информационной безопасностью вычислительных сетей
	ИПК-1.4. Использует криптографическое методы защиты информации в автоматизированных системах	использовать криптографические методы и средства защиты информации в автоматизированных системах	применения средств криптографической защиты информации в автоматизированных системах
	ИПК-1.5. Управляет защитой информации в автоматизированных системах	классифицировать и оценивать угрозы безопасности информации; определять подлежащие защите информационные ресурсы автоматизированных систем; конфигурировать параметры системы защиты информации автоматизированных систем	составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе; устранения неисправностей в работе системы защиты информации автоматизированной системы
ПК-2. Способен учитывать и использовать особенности информационных	ИПК-2.1. Устанавливает и налаживает средства защиты информации в автоматизированных системах	администрировать программные средства системы защиты информации автоматизированных систем	установки и настройки технических и программных средств системы защиты информации

технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации			автоматизированной системы
	ИПК-2.2. Обеспечивает безопасность информационных технологий, применяемых в автоматизированных системах	классифицировать и оценивать угрозы безопасности информации автоматизированной системы; разрабатывать предложения по совершенствованию системы управления защитой информации автоматизированной системы	проведения анализа уязвимостей автоматизированных и информационных систем
ПК-3. Способен учитывать и использовать особенности средств защиты информации при формировании системы защиты информации автоматизированных систем	ИПК-3.1. Проводит анализ уязвимости программных и программно-аппаратных средств системы защиты информации и экспертизу состояния защищенности информации автоматизированных систем с использованием современного инструментария и интеллектуальных информационно-аналитических систем	анализировать защищенность информации автоматизированных систем с использованием современного инструментария и интеллектуальных информационно-аналитических систем;	анализа состояния защищенности информации автоматизированных систем и выработки рекомендаций для принятия решения о модернизации системы защиты информации автоматизированной системы
	ИПК-3.2. Учитывает особенности средств защиты информации при проектировании системы защиты информации	анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных	проектирования системы защиты информации с учетом особенностей средств защиты информации

		уязвимостей безопасности информации в автоматизированных системах	
ПК-4. Способен планировать и организовывать комплекс мероприятий и разрабатывать организационно-распорядительную документацию по защите информации	ИПК-4.1. Разрабатывает организационно-распорядительные документы по защите информации в автоматизированных системах	определять состав и разрабатывать организационно-распорядительные документы по защите информации в автоматизированных системах	подготовки организационно-распорядительной документации определяющей правила и процедуры управления системой защиты информации автоматизированной системы, мониторинга обеспечения уровня защищенности информации автоматизированной системы, защиты информации при выводе автоматизированной системы из эксплуатации, реагирования на инциденты
	ИПК-4.2. Внедряет организационные меры по защите информации в автоматизированных системах	Осуществлять планирование и организацию работы персонала автоматизированной системы с учетом требований по защите информации; Реализовывать правила разграничения доступа персонала к объектам доступа	проведения проверки полноты описания в организационно-распорядительных документах на автоматизированную систему действий персонала по реализации организационны

			х мер защиты информации; подготовки документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации, определяющих правила и процедуры выявления инцидентов, определяющих правила и процедуры управления конфигурацией аттестованной информационной системой и системой защиты информации информационной системы

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 9 зачетных единиц.

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: 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.