государственное бюджетное профессиональное образовательное учреждение
«Пермский химико-технологический техникум»
(ГБПОУ «ПХТТ»)

Одобрено на заседании ПЦК
Информационных технологий и
программирования
Протокол № 9 от 13.06.2018

УТВЕРЖДАЮ
Заместитель директора
О.В.Князева

РАБОЧАЯ ПРОГРАММА
ПРЕДДИПЛОМНОЙ ПРАКТИКИ

для специальности
10.02.05 Обеспечение информационной безопасности автоматизированных систем

2018

Рабочая программа преддипломной практики разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности среднего профессионального образования (далее - СПО) **10.02.05 Обеспечение информационной безопасности автоматизированных систем**, утверждённым приказом Министерства образования и науки Российской Федерации 09 декабря 2016 № 1553, входящим в укрупнённую группу ТОП-50 10.00.00 Информационная безопасность

Организация-разработчик: государственное бюджетное профессиональное образовательное учреждение «Пермский химико-технологический техникум» (ГБПОУ «ПХТТ»**)**

Разработчик:

Жигалова Е. А.

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРЕДДИПЛОМНОЙ ПРАКТИКИ

1.1. Область применения программы:

Рабочая программа преддипломной практики является частью основной профессиональной образовательной программы в соответствии с ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности атвоматизированных систем

в части освоения квалификации техник по защите информации, видов профессиональной деятельности (ВПД) и соответствующих профессиональных компетенций (ПК):

ВПД 1 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.

ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.

ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.

ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.

ВПД 2 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.

ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.

ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.

ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.

ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

ВПД 3 Защита информации техническими средствами

ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.

ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.

ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа.

ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.

ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации.

1.2. Цели и задачи практики

Цели и задачи преддипломной практики:

Преддипломная практика направлена на углубление первоначального практического опыта обучающегося, развитие общих и профессиональных

компетенций, проверку его готовности к самостоятельной трудовой деятельности, а также на подготовку к выполнению выпускной квалификационной работы в организациях различных организационно-правовых форм.

Требования к результатам освоения преддипломной практики

В зависимости от темы выпускной квалификационной работы обучающимися могут быть продемонстрированы результаты освоения одного или несколько ВПД и соответствующих профессиональных компетенций.

ВПД 1 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

иметь практический опыт в:

– эксплуатации компонентов систем защиты информации автоматизированных систем, их диагностике, устранении отказов и восстановлении работоспособности;

– администрировании автоматизированных систем в защищенном исполнении;

– установке компонентов систем защиты информации автоматизированных информационных систем.

уметь:

– обеспечивать работоспособность, обнаруживать и устранять неисправности, осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем;

– производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы;

– организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней;

– настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам.

знать:

– состав и принципы работы автоматизированных систем, операционных систем и сред;

– принципы разработки алгоритмов программ, основных приемов программирования;

– модели баз данных;

– принципы построения, физические основы работы периферийных устройств, основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации;

– теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации;

– порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях.

ВПД 2 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

иметь практический опыт в:

– установке и настройке программных средств защиты информации;

– тестировании функций, диагностике, устранении отказов и восстановлении работоспособности программных и программно-аппаратных средств защиты информации;

– учете, обработке, хранении и передаче информации, для которой установлен режим конфиденциальности.

уметь:

– устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;

– диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;

– проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;

– использовать типовые программные криптографические средства, в том числе электронную подпись;

– устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;

– осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

знать:

– особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;

– типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;

– типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа;

– основные понятия криптографии и типовых криптографических методов и средств защиты информации.

ВПД 3 Защита информации техническими средствами

иметь практический опыт в:

– выявлении технических каналов утечки информации;

– применении, техническом обслуживании, диагностике, устранении отказов, восстановлении работоспособности, установке, монтаже и настройке инженерно-технических средств физической защиты и технических средств защиты информации;

– проведении измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;

– проведении измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.

уметь:

– применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;

– применять технические средства для криптографической защиты информации конфиденциального характера;

– применять технические средства для уничтожения информации и носителей информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных;

– применять инженерно-технические средства физической защиты объектов информатизации.

знать:

– физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;

– номенклатуру и характеристики аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок (далее -

ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;

– основные принципы действия и характеристики, порядок технического обслуживания, устранение неисправностей и организацию ремонта технических средств защиты информации;

– основные способы физической защиты объектов информатизации;

– методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;

– номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам и физической защиты объектов информатизации.

1.3. Количество недель (часов) на освоение рабочей программы преддипломной практики:

Всего:

– преддипломная практика – 4 недели (144 часа);

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОГРАММЫ ПРЕДДИПЛОМНОЙ ПРАКТИКИ

Результатом освоения рабочей программы преддипломной практики в организациях различных организационно-правовых форм, является сформированность профессиональных (ПК) и общих (ОК) компетенций по избранной специальности, собранный материал к выпускной квалификационной работе в соответствии с выбранной тематикой, готовность обучающихся к самостоятельной деятельности по специальности.

Код компе-тенции	Требования компетенции	Наименование результата освоения практики
ПК 1.1.	Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	установка и настройка компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации
ПК 1.2	Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.	администрирование программных и программно-аппаратных компонентов автоматизированной (информационной) системы в защищенном исполнении.
ПК 1.3	Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	обеспечение бесперебойной работы автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.4	Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.	проверка технического состояния, техническое обслуживание и текущий ремонт, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении.
ПК 2.1	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	установка и настройка отдельных программных, программно-аппаратных средств защиты информации.

ПК 2.2.	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	защита информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
ПК 2.3	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.	тестирование функций отдельных программных и программно-аппаратных средств защиты информации.
ПК 2.4.	Осуществлять обработку, хранение и передачу информации ограниченного доступа.	осуществление обработки, хранение и передачу информации ограниченного доступа.
ПК 2.5	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.	уничтожение информации и носителей информации с использованием программных и программно-аппаратных средств.
ПК 2.6.	Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.	оуществление регистрации основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждение и ликвидация последствий компьютерных атак.
ПК 3.1.	Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.	осуществление установки, монтажа, настройки и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.2.	Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.	осуществление эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.3.	Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа	измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа
ПК 3.4.	Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.	измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.
ПК 3.5.	Организовывать отдельные работы по физической защите объектов	организация отдельных работ по физической защите объектов

	информатизации.	информатизации.
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	распознает задачу и/или проблему в профессиональном контексте; анализирует задачу и/или проблему и выделяет её составные части; определяет этапы решения задачи; выявляет и осуществляет поиск информации, необходимой для решения задачи и/или проблемы; составляет план действия; определяет необходимые ресурсы; владеет актуальными методами работы в профессиональной и смежных сферах; реализует составленный план; оценивает результат и последствия своих действий, выделяет в нём сильные и слабые стороны
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	определяет задачи поиска информации; определяет необходимые источники информации; планирует процесс поиска; структурирует получаемую информацию в соответствии с параметрами поиска; выделяет наиболее значимое в перечне информации; оценивает практическую значимость результатов поиска; интерпретирует полученную информацию в контексте профессиональной деятельности; оформляет результаты поиска
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие.	использует актуальную нормативно-правовую документацию по специальности; применяет современную научно профессиональную терминологию; определяет актуальность нормативно-правовой документации в профессиональной деятельности; выстраивает траектории

		профессионального и личностного развития; участвует в конкурсах профессионального мастерства; участвует в мероприятиях профессиональной направленности (вебинары, семинары, конференции, круглые столы, форумы и т.д.)
ОК 4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	участвует в деловом общении для эффективного решения деловых задач; планирует профессиональную деятельность; организует работу коллектива и команды; взаимодействует с коллегами, руководством, клиентами; при групповом обсуждении задает вопросы для понимания идей других; при групповом обсуждении: убеждается, что коллеги по группе поняли предложенную идею; участвует в деятельности по выявлению ресурсов команды; анализирует работу членов группы; анализирует результаты выполненного задания; презентует результаты работы группы; защищает полученные командой результаты.
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	грамотно (устно и письменно) излагает свои мысли по профессиональной тематике на государственном языке; проявляет толерантность в рабочем коллективе; извлекает из устной речи (монолог, диалог, дискуссия) нужную информацию и логические связи, организующие эту информацию; грамотно оформляет документы на государственном языке; корректно общается с преподавателями и одногруппниками; соблюдает заданный жанр

		высказывания (служебный доклад, выступление на совещании / собрании, презентация товара / услуг); корректно отвечает на вопросы, направленные на выяснение мнения (позиции); задает четко сформулированные вопросы, направленные на получение необходимой информации.
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.	соблюдает нормы поведения во время учебных занятий и прохождения учебной и производственной практик; понимать значимость своей специальности; демонстрирует поведение на основе общечеловеческих ценностей
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	эффективность выполнения правил техники безопасности во время учебных занятий, при прохождении учебной и производственной практик; использует ресурсосберегающие технологии в профессиональной деятельности, на рабочем месте.
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.	Использовать физкультурно-оздоровительную деятельность для укрепления здоровья, достижения жизненных и профессиональных целей; применять рациональные приемы двигательных функций в профессиональной деятельности; пользоваться средствами профилактики перенапряжения характерными для данной специальности
ОК 9.	Использовать информационные технологии в профессиональной деятельности.	ориентируется в информационно-коммуникационных технологиях, применяемых в профессиональной деятельности; применяет средства информатизации и информационных технологий для реализации профессиональной деятельности; в профессиональной деятельности использует

		современное программное обеспечение; представляет информацию в различных формах с использованием разнообразного программного обеспечения; способен адаптироваться в новых программных продуктах.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.	понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые); понимает тексты на базовые профессиональные темы; применяет в профессиональной деятельности инструкции на государственном и иностранном языке; строит простые высказывания о себе и о своей профессиональной деятельности; пишет простые связные сообщения на знакомые или интересующие профессиональные темы.

3. ТЕМАТИЧЕСКИЙ ПЛАН И СОДЕРЖАНИЕ ПРЕДДИПЛОМНОЙ ПРАКТИКИ

3.1. Тематический план практики

Коды профессиональных общих компетенций	**Наименования разделов профессионального модуля**	**производственная практика, часов**
ПК 1.1- ПК.1.4 ПК 2.1- ПК 2.6 ПК 3.1- ПК 3.6 ОК 1– ОК10	**Преддипломная практика**	**144**
	Всего преддипломной практики	**144**
	Консультации	**0**
	Промежуточная аттестация	**0**
	Всего	**144**

3.2. Содержание практики

Наименование разделов профессионального модуля (ПМ) и профессиональных компетенций	Содержание работ		Объем часов
1	2		3
ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации. ПК 1.2. Администрировать программные и	**Производственная (преддипломная) практика** Виды работ		**144**
	1	Общее ознакомление со структурой и работой предприятия.	6
	2	Изучение обязанностей персонала, осуществляющего обеспечение информационной безопасности автоматизированных систем	12
	3	Выполнение обязанностей персонала по одной из должностей,	114

программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.		связанных с обеспечение информационной безопасности автоматизированных систем. Подбор материалов по заданию на выпускную квалификационную работу.	
ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации. ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении. ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации. ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами. ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации. ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа. ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств. ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием	4	Составление отчетной документации по практике.	9

программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак. ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации. ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации. ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа. ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации. ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации.			
	5	Защита отчета по практике	3
		Итого	144

4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ПРЕДДИПЛОМНОЙ ПРАКТИКИ

4.1. Требования к минимальному материально-техническому обеспечению

Реализация рабочей программы преддипломной практики предполагает наличие на предприятии рабочих мест на базе вычислительной техники, подключенные к локальной вычислительной сети и информационно-телекоммуникационной сети Интернет;

- Программное обеспечение общего и профессионального назначения
- Оборудование для установки, монтажа, настройки и технического обслуживания технических средств защиты информации
- Оборудование для организации отдельных видов работ по физической защите объектов информатизации

4.2. Информационное обеспечение практики

Основные источники

1. Батаев А.В. Операционные системы и среды: учебник для студентов СПО / А.В. Батаев, Н.Ю., Налютин, С.В. Синицын. - М.: Издательский центр "Академия", 2015г.
2. Батаев А.В. Операционные системы и среды: учебник для студентов СПО / А.В. Батаев, Н.Ю., Налютин, С.В. Синицын. - М.: Издательский центр "Академия", 2017г.
3. Кумскова И.А. Базы данных: учебник для студентов учреждений среднего профессионального образования. – М.: КНОРУС, 2018г.
4. Кумскова И.А. Базы данных: учебник / Кумскова И.А. — Москва: КноРус, 2021. — 400 с. — ISBN 978-5-406-08303-1. — URL: https://book.ru/book/940108 (дата обращения: 23.04.2021). — Текст: электронный.
5. Мартишин С.А. Базы данных. Практическое применение СУБД SGL и NOSGL-типа для проектирования информационных систем: учебное пособие для студентов высших учебных заведений /С.А. Мартишин, В.Л. Симонов, М.В. Храпченко. – М.: ИД «ФОРУМ»: ИНФРА-М, 2017г.
6. Чулюков В.А. Проектирование баз данных. Практический курс: учебное пособие / Чулюков В.А., Астахова И.Ф., Башарина С.О., Сидорова О.А. — Москва: Русайнс, 2020. — 163 с. — ISBN 978-5-4365-5748-9. — URL: https://book.ru/book/938011 (дата обращения: 23.04.2021). — Текст: электронный.
7. Костров Б.В. Сети и системы передачи информации: учебник для студентов учреждений среднего профессионального образования / Б.В. Костров, В.Н. Ручкин. – М.: Издательский центр «Академия», 2017г.

8. Гагарина Л.Г. Разработка и эксплуатация автоматизированных информационных систем: учебное пособие для студентов СПО. – М.: ИД «ФОРУМ»: ИНФРА-М, 2016г.
9. Гвоздева В.А. Основы построения автоматизированных информационных систем: учебник для студентов СПО. – М.: ИД «ФОРУМ»: ИНФРА-М, 2015г.
10. Дергачев К.В. Защита информации: лабораторный практикум: учебное пособие / Дергачев К.В., Титарев Д.В. — Москва: Русайнс, 2021. — 158 с. — ISBN 978-5-4365-6774-7. — URL: https://book.ru/book/940250 (дата обращения: 23.04.2021). — Текст: электронный.
11. Программно-аппаратные средства обеспечения информационной безопасности: учебное пособие для студентов высших учебных заведений / А.В. Душкин, О.М. Барсуков, Е.В. Кравцов, К.В., Славнов. – М.: Горячая линия – Телеком, 2018г.
12. Сагдеев К.М. Физические основы защиты информации Бакалавриат: учебное пособие / Сагдеев К.М., Петренко В.И., Чипига А.Ф. — Ставрополь: Северо-Кавказский федеральный университет, 2015. — 394 с. — URL: https://book.ru/book/928736 (дата обращения: 23.04.2021). — Текст: электронный.
13. Бабаш А.В. Криптографические методы защиты информации: учебник / Бабаш А.В., Баранова Е.К. — Москва: КноРус, 2020. — 189 с. — ISBN 978-5-406-00169-1. — URL: https://book.ru/book/933943 (дата обращения: 23.04.2021). — Текст: электронный.
14. Баранова Е.К. Криптографические методы защиты информации. Лабораторный практикум +CD: учебное пособие / Баранова Е.К., Бабаш А.В. — Москва: КноРус, 2017. — 196 с. — (для бакалавров). — ISBN 978-5-406-03802-4. — URL: https://book.ru/book/920017 (дата обращения: 23.04.2021). — Текст: электронный.
15. Баричев С.Г. Основы современной криптографии: учебный курс для студентов высших учебных заведений / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов. – М.: Горячая линия-Телеком, 2017г.
16. Криптографические методы защиты информации: лабораторный: практикум / сост. Калмыков И.А., Науменко Д.О., Гиш Т.А. — Ставрополь: Северо-Кавказский федеральный университет, 2015. — 109 с. — URL: https://book.ru/book/928786 (дата обращения: 23.04.2021). — Текст: электронный.
17. Скрипник Д.А. Общие вопросы технической защиты информации: курс лекций / Скрипник Д.А. — Москва: Интуит НОУ, 2016. — 424 с. — URL: https://book.ru/book/917804 (дата обращения: 23.04.2021). — Текст: электронный.
18. Москвитин Г.И. Комплексная защита информации в организации: монография / Москвитин Г.И. — Москва: Русайнс, 2020. — 354 с. — ISBN 978-5-4365-1561-8. — URL: https://book.ru/book/934814 (дата обращения: 23.04.2021). — Текст: электронный.

19. Сагдеев К.М. Физические основы защиты информации Бакалавриат: учебное пособие / Сагдеев К.М., Петренко В.И., Чипига А.Ф. — Ставрополь: Северо-Кавказский федеральный университет, 2015. — 394 с. — URL: https://book.ru/book/928736 (дата обращения: 23.04.2021). — Текст: электронный.

Дополнительные источники:

1. Вильямс Р. Mac OS X 10.5 Leopard: учебное пособие. - СПб: БХВ-Петербург, 2013г.
2. Назаров С.В. Операционные системы. Практикум: учебное пособие / Назаров С.В., Гудыно Л.П., Кириченко А.А. — Москва: КноРус, 2020. — 372 с. — ISBN 978-5-406-07707-8. — URL: https://book.ru/book/933567 (дата обращения: 22.04.2021). — Текст: электронный.
3. Назаров С.В. Современные операционные системы: курс лекций / Назаров С.В., Широков А.И. — Москва: Интуит НОУ, 2016. — 351 с. — ISBN 978-5-9963-0416-5. — URL: https://book.ru/book/918225 (дата обращения: 22.04.2021). — Текст: электронный.
4. Агальцов В.П. Базы данных. В 2-х кн.: учебник для высших учебных заведений. – М.: ИД «ФОРУМ»: ИНФРА-М, 2014г.
5. Астахова И.Ф. Объектные базы данных: учебное пособие / Астахова И.Ф., Борисенков Д.В., Киселева Е.И., Самойлов Н.К. — Москва: Русайнс, 2020. — 93 с. — ISBN 978-5-4365-5404-4. — URL: https://book.ru/book/936907 (дата обращения: 23.04.2021). — Текст: электронный.
6. Кондрашов Ю.Н. Язык SQL. Сборник ситуационных задач по дисциплине «Базы данных: учебно-практическое пособие / Кондрашов Ю.Н. — Москва: Русайнс, 2020. — 125 с. — ISBN 978-5-4365-4598-1. — URL: https://book.ru/book/935744 (дата обращения: 23.04.2021). — Текст: электронный.
7. Литвинская О.С. Основы теории передачи информации: учебное пособие / Литвинская О.С., Чернышев Н.И. — Москва: КноРус, 2021. — 168 с. — ISBN 978-5-406-08653-7. — URL: https://book.ru/book/940469 (дата обращения: 23.04.2021). — Текст: электронный.
8. Мезенцев К.Н. Автоматизированные информационные системы: учебник для студентов СПО. - М.: Издательский центр "Академия", 2014г.
9. Руденков Н.А. Технологии защиты информации в компьютерных сетях: курс лекций / Руденков Н.А., Пролетарский А.В., Смирнова Е.В., Суровов А.М. — Москва: Интуит НОУ, 2016. — 368 с. — URL: https://book.ru/book/918258 (дата обращения: 23.04.2021). — Текст: электронный
10. Варлатая С.К. Защита информационных процессов в компьютерных сетях: учебно-методическое пособие / Варлатая С.К., Шаханова М.В. —

Москва: Проспект, 2015. — 216 с. — ISBN 978-5-392-19174-1. — URL: https://book.ru/book/918021 (дата обращения: 23.04.2021). — Текст: электронный.

11. Новожилов Е.О. Компьютерные сети: учебное пособие для студентов средних профессиональных учебных заведений. - М.: Издательский центр "Академия", 2014г.
12. Руденков Н.А. Технологии защиты информации в компьютерных сетях: курс лекций / Руденков Н.А., Пролетарский А.В., Смирнова Е.В., Суровов А.М. — Москва: Интуит НОУ, 2016. — 368 с. — URL: https://book.ru/book/918258 (дата обращения: 23.04.2021). — Текст: электронный.
13. Смирнова Е.В. Построение коммутируемых компьютерных сетей: курс лекций / Смирнова Е.В., Баскаков И.В., Пролетарский А.В., Федотов Р.А. — Москва: Интуит НОУ, 2016. — 428 с. — URL: https://book.ru/book/917979 (дата обращения: 23.04.2021). — Текст: электронный
14. Москвитин Г.И. Комплексная защита информации в организации: монография / Москвитин Г.И. — Москва: Русайнс, 2020. — 354 с. — ISBN 978-5-4365-1561-8. — URL: https://book.ru/book/934814 (дата обращения: 23.04.2021). — Текст: электронный.
15. Нестандартные методы защиты информации: лабораторный: практикум / сост. Пашинцев В.П., Ляхов А.В. — Ставрополь: Северо-Кавказский федеральный университет, 2016. — 196 с. — URL: https://book.ru/book/928802 (дата обращения: 23.04.2021). — Текст: электронный.
16. Тараскин М.М. Комплексная защита информации в организации: монография / Тараскин М.М., и др. — Москва: Русайнс, 2017. — 353 с. — ISBN 978-5-4365-1561-8. — URL: https://book.ru/book/922538 (дата обращения: 23.04.2021). — Текст: электронный.
17. Царегородцев А.В. Методы и средства защиты информации в государственном управлении: учебное пособие / Царегородцев А.В., Тараскин М.М. — Москва: Проспект, 2017. — 205 с. — ISBN 978-5-392-20353-6. — URL: https://book.ru/book/922352 (дата обращения: 23.04.2021). — Текст: электронный.
18. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие для студентов СПО. - М.: ИД "ФОРУМ": ИНФРА-М, 2016г.
19. Мельников В.П. Информационная безопасность: учебное пособие для студентов средних профессиональных учебных заведений. - М.: Издательский центр "Академия", 2010г.
20. Гребенюк Е.И. Технические средства информатизации: учебник для студентов СПО / Е.И. Гребенюк, Н.А. Гребенюк. - М.: Издательский центр "Академия", 2014г.

21. Лавровская О.Б. Технические средства информатизации. Практикум: учебное пособие для студентов СПО. - М.: Издательский центр "Академия", 2013г.
22. Руденков Н.А. Технологии защиты информации в компьютерных сетях : курс лекций / Руденков Н.А., Пролетарский А.В., Смирнова Е.В., Суровов А.М. — Москва : Интуит НОУ, 2016. — 368 с. — URL: https://book.ru/book/918258 (дата обращения: 23.04.2021). — Текст: электронный
23. Тараскин М.М. Комплексная защита информации в организации: монография / Тараскин М.М., и др. — Москва: Русайнс, 2017. — 353 с. — ISBN 978-5-4365-1561-8. — URL: https://book.ru/book/922538 (дата обращения: 23.04.2021). — Текст: электронный

Интернет-ресурсы:

1. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
2. Информационный портал по безопасности www.SecurityLab.ru.
3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
4. Российский биометрический портал www.biometrics.ru
5. Сайт журнала Информационная безопасность http://www.itsec.ru –
6. Сайт Научной электронной библиотеки www.elibrary.ru
7. Справочно-правовая система «Гарант» » www.garant.ru
8. Справочно-правовая система «Консультант Плюс» www.consultant.ru
9. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
10. Федеральный портал «Информационно-коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
11. Федеральный портал «Российское образование www.edu.ru
12. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
13. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
14. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
15. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/
16. Федеральный портал «Информационно- коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
17. Сайт Научной электронной библиотеки www.elibrary.ru

4.3. Общие требования к организации преддипломной практики

Преддипломная практика проводится непрерывно после освоения учебной практики и практики по профилю специальности.

Практика проводится в профильных организациях на основе договоров, заключаемых между образовательной организацией и профильными организациями. В договоре Техникум и Организация оговаривают все вопросы, касающиеся проведения практики.

Консультирование по выполнению заданий, контроль посещения мест преддипломной практики, проверка отчетов по итогам практики и выставление оценок осуществляется руководителем практики от техникума.

Общее руководство практикой осуществляет ответственный за производственную практику. Ответственный за организацию практики утверждает общий план её проведения, оформляет проект распорядительного акта руководителя образовательной организации или иного уполномоченного им лица с указанием закрепления каждого обучающегося за профильной организацией, а также с указанием вида и сроков прохождения практики.

Перед началом практики проводится организационное собрание с целью ознакомления студентов с приказом, сроками практики, порядком организации работы во время практики в организации, оформлением необходимой документации, правилами техники безопасности, распорядком дня, видами и сроками отчетности и т.п.

Преддипломная практика является завершающим этапом освоения ООП и завершается дифференцированным зачетом (зачетом) при условии положительного аттестационного листа по практике руководителей практики от профильной организации и образовательной организации об уровне освоения профессиональных компетенций; наличия положительной характеристики профильной организации на обучающегося по освоению общих компетенций в период прохождения практики; полноты и своевременности представления дневника практики и отчета о практике в соответствии с заданием на практику.

Результаты прохождения практики представляются обучающимся в образовательную организацию и учитываются при прохождении государственной итоговой аттестации.

Обучающиеся, не прошедшие практику или получившие отрицательную оценку, не допускаются к прохождению государственной итоговой аттестации.

4.4. Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических (инженерно-педагогических) кадров, осуществляющих проведение практики:

Квалификация педагогических работников образовательной организации должна отвечать квалификационным требованиям, указанным в квалификационных справочниках, и (или) профессиональных стандартах (при наличии). Инженерно-педагогический состав: дипломированные специалисты, направление деятельности которых соответствует области профессиональной деятельности или преподаватели междисциплинарных курсов, а также общепрофессиональных дисциплин и профессиональных модулей по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)

Контроль и оценка результатов освоения преддипломной практики осуществляется руководителем практики в процессе самостоятельного выполнения обучающимися заданий.

Текущий контроль проводится руководителем практики в процессе выполнения обучающимися индивидуальных заданий, проектов, исследований.

Формы и методы текущего контроля доводятся до сведения обучающихся на организационном собрании по практике.

Дифференцированный зачет проходит в форме защиты отчета по преддипломной практике в последний день практики.