Министерство образования и молодежной политики Свердловской области
государственное автономное профессиональное образовательное учреждение
Свердловской области «Уральский радиотехнический колледж им. А.С. Попова»

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.02 Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах

для специальности среднего профессионального образования
10.02.03 Информационная безопасность автоматизированных систем
базового уровня подготовки

2020 г.

Рабочая программа профессионального модуля разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования

10.02.03 Информационная безопасность автоматизированных систем

УТВЕРЖДАЮ
Заместитель директора
по учебной работе
_____ Д.В. Колесников

«30» июня 2020 г.

Рекомендована цикловой методической комиссией
«Электронных вычислительных машин»
Протокол от « 29 » июня 2020 г. № 6

Председатель ЦМК _____ Ю.Г. Котова

Разработчики:

Уймин А.Г., преподаватель УРТК им. А. С. Попова

СОДЕРЖАНИЕ

1 ПАСПОРТ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ 4

2 РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ 7

3 СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ 9

4 УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ 22

5 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ВИДА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ) 26

1 ПАСПОРТ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.02 Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах

1.1 Область применения программы

Рабочая программа профессионального модуля является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности СПО 10.02.03 «Информационная безопасность автоматизированных систем» базового уровня подготовки в части освоения основного вида профессиональной деятельности (ВПД) «Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах» и соответствующих профессиональных компетенций (ПК):

– ПК 2.1. Применять программно-аппаратные средства обеспечения информационной безопасности в автоматизированных системах.

– ПК 2.2. Участвовать в эксплуатации программно-аппаратных средств обеспечения информационной безопасности, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности.

– -ПК 2.3. Участвовать в мониторинге эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах.

– -ПК 2.4. Участвовать в обеспечении учета, обработки, хранения и передачи конфиденциальной информации.

– ПК 2.5. Решать частные технические задачи, возникающие при проведении всех видов плановых и внеплановых контрольных проверок, при аттестации объектов, помещений, программ, алгоритмов.

– ПК 2.6. Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности программно-аппаратными средствами.

1.2 Цели и задачи модуля – требования к результатам освоения модуля

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения профессионального модуля должен:

иметь практический опыт:

– применения программно-аппаратных средств обеспечения информационной безопасности;

– диагностики, устранения отказов и восстановления работоспособности программно-аппаратных средств обеспечения информационной безопасности;

– мониторинга эффективности программно-аппаратных средств обеспечения информационной безопасности;

– обеспечения учета, обработки, хранения и передачи конфиденциальной информации;

– решения частных технических задач, возникающих при аттестации объектов, помещений, программ, алгоритмов;

– применения нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами;

уметь:

– применять программно-аппаратные средства обеспечения информационной безопасности;

– диагностировать, устранять отказы и обеспечивать работоспособность программно-аппаратных средств обеспечения информационной безопасности;

– оценивать эффективность применяемых программно-аппаратных средств обеспечения информационной безопасности;

– участвовать в обеспечении учета, обработки, хранения и передачи конфиденциальной информации;

– решать частные технические задачи, возникающих при аттестации объектов, помещений, программ, алгоритмов;

– использовать типовые криптографические средства и методы защиты информации, в том числе и электронную цифровую подпись;

– применять нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности программно-аппаратными средствами;

знать:

– методы и формы применения программно-аппаратных средств обеспечения информационной безопасности;

– особенности применения программно-аппаратных средств обеспечения информационной безопасности в операционных системах, компьютерных сетях, базах данных;

– типовые модели управления доступом;

– типовые средства, методы и протоколы идентификации, аутентификации и авторизации;

– типовые средства и методы ведения аудита и обнаружения вторжений;

– типовые средства и методы обеспечения информационной безопасности в локальных и глобальных вычислительных сетях;

– основные понятия криптографии и типовые криптографические методы защиты информации

1.3 Количество часов на освоение программы профессионального модуля:

всего – 1361 час, в том числе:

- максимальной учебной нагрузки обучающегося 821 час, включая:
  - обязательной аудиторной учебной нагрузки обучающегося –558 часов;
  - самостоятельной работы обучающегося – 263 часа;
- учебная практика 144 часа;
- производственная практика по профессии – 396 часов.

2 РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения рабочей программы профессионального модуля является овладение обучающимися видом профессиональной деятельности «Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах», в том числе профессиональными (ПК) и общими (ОК) компетенциями:

Код	Наименование результата обучения
ПК 2.1	Применять программно-аппаратные средства обеспечения информационной безопасности в автоматизированных системах.
ПК 2.2	Участвовать в эксплуатации программно-аппаратных средств обеспечения информационной безопасности, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности.
ПК 2.3	Участвовать в мониторинге эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах.
ПК 2.4	Участвовать в обеспечении учета, обработки, хранения и передачи конфиденциальной информации.
ПК 2.5	Решать частные технические задачи, возникающие при проведении всех видов плановых и внеплановых контрольных проверок, при аттестации объектов, помещений, программ, алгоритмов.
ПК 2.6	Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности программно-аппаратными средствами.
ОК 1	Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности.
ОК 2	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
ОК 3	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
ОК 4	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
ОК 5	Использовать информационно-коммуникационные технологии в профессиональной деятельности.
ОК 6	Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.
ОК 7	Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.
ОК 8	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

Код	Наименование результата обучения
ОК 9	Ориентироваться в условиях частой смены технологий в профессиональной деятельности.
ОК 10	Формулировать задачи логического характера и применять средства математической логики для их решения.
ОК 11	Владеть основными методами и средствами разработки программного обеспечения.
ОК 12	Производить инсталляцию и настройку автоматизированных информационных систем, выполнять в автоматизированных информационных системах регламентные работы по обновлению, техническому сопровождению и восстановлению при отказах.

3 СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ. 02 «Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах»

3.1 Тематический план профессионального модуля

Коды профессиональных компетенций	**Наименования разделов профессионального модуля***	**Всего часов**	**Объем времени, отведенный на освоение междисциплинарного курса (курсов)**					**Практика**	
			Обязательная аудиторная учебная нагрузка обучающегося			**Самостоятельная работа обучающегося**		**Учебная,** часов	**Производственная (по профилю специальности),** часов
			Всего, часов	**в т.ч. лабораторные работы и практические занятия,** часов	**в т.ч., курсовая работа (проект),** часов	**Всего,** часов	**в т.ч., курсовая работа (проект),** часов		
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
ПК 2.1 - ПК 2.6.	**Раздел 1 Применение программно – аппаратных средств обеспечения информационной безопасности**	**708**	**380**	150	30 -	**184**	26	**144**	**-**
ПК 2.3, ПК 2.4	**Раздел 2 Применение криптографических средств и методов защиты информации**	**194**	**136**	58		**58**	-	**-**	
ПК 2.6	**Раздел 3 Применение метрологии, стандартизации и сертификации на предприятиях**	**63**	**42**	10		**21**	-		
ПК 2.1 - ПК 2.6.	**Производственная практика (по профилю специальности)**, часов	**396**							**396**
	Всего:	**1361**	**558**	218	30	**263**	26	**144**	**396**

3.2Содержание обучения по профессиональному модулю (ПМ)

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)		Объем часов	Уровень освоения
1	**2**		**3**	**4**
Раздел 1 Применение программно – аппаратных средств обеспечения информационной безопасности			**708**	
МДК.02.01 Программно-аппаратные средства обеспечения информационной безопасности			**564**	
Тема 1.1 Основы виртуальных частных сетей	**Содержание**		20	
	1.	Протокол GRE		2
	2.	Виртуальные частные сети		2
	3.	Протоколы канального уровня		2
	4.	Point-to-Point Protocol (PPP)		2
	5.	Конфигурация LCP		2
	6.	Способы передачи PPP по Ethernet		2
	7.	Формат AVP		2
	8.	Установление управляющего соединения		2
	9.	Состояния управляющего соединения		2
	10.	Обсуждение безопасности		2
	Лабораторные работы		4	
	1.	Настройка PPP сервера		
	2.	Настройка PPP клиента		
Тема 1. 2 Семейство протоколов IPSec	**Содержание**		32	
	1.	Семейство протоколов IPSec		2
	2.	Протокол AH		2
	3.	Протокол ESP		2
	4.	Понятие домена IPSec		2
	5.	Степень детализации управления трафиком		2
	6.	База данных безопасной ассоциации (SAD)		2
	7.	Формат сообщений		2
	8.	Протокол IKE		2
	9.	Использование NAT в протоколе IPSec		2

1	2		3	4
	10.	Сравнение keepalive и heartbeat		2
	11.	Совместное использование протоколов L2TP и IPSec		2
	12.	Начальные записи в политике, необходимые для защиты SCCRQ		2
	13.	Протокол SSL/TLS, Протокол записи, протокол рукопожатия		2
	14.	Добавление дополнительных возможностей в протокол		2
	Лабораторные работы		26	
	1.	Настройка NAT		
	2.	Настройка NAT Pool		
	3.	Настройка SAT, PAT		
	4.	Настройка DNS Relay		
	5.	Развертывание виртуальной частной сети на базе технологии IPSec на базе программного сервера		
	6.	Развертывание виртуальной частной сети на базе технологии PPTP		
	7.	Развертывание виртуальной частной сети на базе технологии L2TP		
	8.	Развертывание виртуальной частной сети на базе технологии SSL		
Дифференцированный зачет			**2**	
Тема 1.3 Средства восстановления данных	**Содержание**		6	
	1.	Коммерческие и некоммерческие средства восстановления информации.		2
	2.	Особенности создания посекторных образов НЖМД.		2
	3.	Средства исследования реестра для ОС Windows и Linux»		2
	Лабораторные работы		8	
	1.	Использование средств foremost и scalpel, расширение баз сигнатур		
	2.	Использование систем R-Studio и EnCase.		
Тема 1. 4 Системы обнаружения вторжений	**Содержание**		20	
	1.	Требования к аппаратным средствам идентификации-аутентификации пользователей, применяемым в ЭЗ и АПМДЗ.		2
	2.	СОВ и системы обнаружения компьютерных атак (СОА).		2
	3.	Отличия в требованиях и функциях СОВ и СОА. Основные архитектуры СОВ.		2
	4.	Аппаратный компонент СОВ (TAP, Span-Port, Bridge, Proxy, HUB). Особенности использования.		2
	5.	Программный компонент СОВ.		2
	6.	Средства восстановления информации прикладного уровня в сетевом трафике на СОВ.		2
	7.	Протоколы в сетях с коммутацией пакетов. Примеры (IPX/SPX, NetBIOS, TCP/IP).		2

1	2		3	4
	8.	Сеть Internet, как сеть с коммутацией пакетов. История, особенности, перспективы развития.		2
	9.	Стек протоколов TCP/IP (4-х уровневая модель DARPA). Особенности маршрутизации в сетях TCP/IP.		2
	10.	Штатные средства защиты информации стека протоколов TCP/IP, средства идентификации-аутентификации на разных уровнях протоколов TCP/IP. Достоинства, недостатки, ограничения.		2
	Лабораторные работы		8	
	1.	Установка и начальное конфигурирование простейших СОА		
	2.	Использование сетевых снифферов в качестве СОВ		
Тема 1.5 Криптографические и некриптографические средства организации VPN	**Содержание**		8	
	1.	Криптографические и некриптографические средства организации VPN.		2
	2.	Необходимое и достаточное условие достижения заранее заданного уровня стойкости VPN.		2
	3.	Различные типы устройств, образующих VPN. Криптомаршрутизаторы и криптофильтры.		2
Тема 1.6 Криптороутер	**Содержание**		8	2
	1.	Криптороутер. Основные принципы, архитектура		
	2.	Криптофильтр. Модель нарушителя. Достоинства, недостатки.		2
Тема 1.7 Межсетевые экраны и системы мониторинга	**Содержание**		68	
	1.	Межсетевые экраны типа Firewall. Достоинства, недостатки, реализуемые политики безопасности.		2
	2.	Основные типы FIREWALL. Симметричные и несимметричные.		2
	3.	Однохостовые Firewall. Достоинства, недостатки.		2
	4.	Мультихостовые Firewall. Достоинства, недостатки.		2
	5.	Требования к каждому хосту МЭ, исходя из архитектуры и выполняемых функций.		2
	6.	Требования по сертификации МЭ типа Firewall ФСТЭК и ФСБ.		2
	7.	Особенности фиксации событий в системах, построенных на разных принципах: сети с коммутацией соединений.		2
	8.	Особенности фиксации событий в системах, построенных на разных принципах: сети с коммутацией пакетов, сети TCP/IP, сети X.25.		2
	9.	Общие уязвимости систем мониторинга и способы обнаружения их работы извне, классификация отслеживаемых событий: атаки, вторжения.		2
	10.	Нарушения политики безопасности: обнаружение вторжений, обнаружение атак (мониторинг внутри и вне ЛВС), особенности построения систем мониторинга.		2

1	2		3	4
	11.	Сетевые мониторы. Режим сканирования трафика: пассивные, актив ные.		2
				2
				2
	12.	Сетевые мониторы. Косвенные, использующие результаты работы сетевых анализаторов и/или других источников		2
	13.	Сетевые мониторы. Режим работы с оборудованием: монопроцессор-ные .		2
	14.	Сетевые мониторы. Режим работы с оборудованием: секционирован-ные (мультисистемные и моносистемные)		2
	15.	Сетевые мониторы. Режим обработки трафика: сигнатурные, эвристи-ческие, смешанные.		2
	16.	Сетевые мониторы. Режим реакции на обнаруженную атаку: исправ-ляющий, обнаруживающий.		2
	17.	Сетевые мониторы: возможность пополнения базы атак: открытые и закрытые;		2
	18.	Сетевые мониторы: возможность обнаружения комплексных атак		2
	19.	Сетевой монитор Real Secure (место в классификации, архитектура, возможности, достоинства и недостатки, уязвимости, рекомендации по установке и администрированию;		2
	20.	Сетевой монитор NFR (место в классификации, архитектура, возмож-ности, достоинства, недостатки).		2
	21.	Сетевой монитор NFR (язык описания событий, рекомендации по установке и администрированию).		2
	22.	Сетевой монитор SNORT (место в классификации, архитектура, воз-можности, достоинства, недостатки).		2
	23.	Сетевой монитор SNORT (язык описания событий, рекомендации по установке и администрированию).		2
	Лабораторные работы		74	
	1.	Уровень 1 - пакетные фильтры		
	2.	Уровень 2 - фильтрация служб с протоколозависимыми модулям и поиск ключевых слов в теле пакетов на сетевом уровне		
	3.	Уровень 3 - proxy сервера прикладного уровня.		
	4.	Фиксация событий в промышленных системах		
	5.	Сетевые мониторы		
	6.	Анализ состояния внутреннего коммутационного оборудования (SNMP)		
	7.	Получение интегральных статистических характеристик о трафике через МЭ		

1	2		3	4
	8.	Внешняя и внутренняя проверка целостности ресурсов общего пользования с применением однонаправленных криптографических преобразований		
	9.	Проверка корректности работы службы имен		
	10.	Проверка скорости реакции ресурсов общего пользования на стохастические запросы		
	11.	Информация от программных агентов рабочих станций и серверов		
	12.	Журналы аудита МЭ		
	13.	Журналы аудита серверов-посредников		
	14.	Журналы аудита серверов-ресурсов общего пользования		
	15.	Журналы систем усиленной идентификации/аутентификации		
	16.	Сравнение типов сетевых мониторов		
	17.	Установка и начальное конфигурирование Real Secure		
	18.	Установка и начальное конфигурирование NFR		
	19.	Установка и начальное конфигурирование SNORT		
Дифференцированный зачет			**2**	
Тема 1.8 СЗИ от НСД	**Содержание**		34	
	1.	Меры противодействия несанкционированному доступу		2
	2.	Идентификация и аутентификация пользователей		2
	3.	Ограничение доступа на вход в систему		2
	4.	Разграничение доступа. Регистрация событий (аудит)		2
	5.	Модель защищенной компьютерной системы		2
	6.	СЗИ от НСД: Общие сведения		2
	7.	СЗИ от НСД: Запуск и регистрация в системе защиты		2
	8.	СЗИ от НСД: Создание пользователей		2
	9.	СЗИ от НСД: Реализация мандатной модели разграничения доступа		2
	10.	СЗИ от НСД: Реализация дискреционной модели разграничения доступа.		2
	11.	СЗИ от НСД: Обеспечение замкнутости программной среды		2
	12.	СЗИ от НСД: Контроль целостности		2
	13.	СЗИ от НСД: Регистрация событий		2
	14.	СЗИ от НСД: Печать штампа		2
	15.	СЗИ от НСД: Гарантированное удаление данных		2
	16.	СЗИ от НСД: Реализация запрета загрузки ПЭВМ в обход СЗИ		2
	17.	СЗИ от НСД: Настройка механизма шифрования		2
	Лабораторные работы		30	
	1.	Система защиты информации от НСД		
	2.	СЗИ от НСД. Запуск и регистрация в системе защиты		
	3.	СЗИ от НСД: Создание пользователей		
	4.	СЗИ от НСД: Реализация выбранной модели разграничения доступа		

1	2		3	4
	5.	СЗИ от НСД: Обеспечение замкнутости программной среды		
	6.	СЗИ от НСД: Контроль целостности		
	7.	СЗИ от НСД: Регистрация событий		
	8.	СЗИ от НСД. Печать штампа		
	9.	СЗИ от НСД. Гарантированное удаление данных		
	10.	СЗИ от НСД. Реализация запрета загрузки ПЭВМ в обход СЗИ		
	11.	СЗИ от НСД. Настройка механизма шифрования		
Курсовое проектирование			30	3
КП1 Оформление задания. Состав пояснительной записки				
КП2. Разработка введения. Требования к разделу.				
КП3. Описание компонентов системы				
КП4. Выбор и обоснование СЗИ от НСД				
КП5. Описание методики настройки				
КП6. Инструменты проверки				
КП7. Запуск и регистрация в системе защиты				
КП8. Создание пользователей				
КП9. Реализация мандатной модели разграничения доступа				
КП10. Реализация дискреционной модели разграничения доступа				
КП11. Обеспечение замкнутости программной среды				
КП12. Контроль целостности. Регистрация событий. Печать штампа.				
КП13. Гарантированное удаление данных				
КП14. Расчёт стоимости работ по обеспечению защиты				
КП15. Расчёт стоимости работ по обеспечению защиты				
Самостоятельная работа при изучении раздела 1 ПМ.02 Систематическая проработка конспектов занятий, учебной литературы по главам и параграфам, указанным преподавателем. Подготовка к лабораторным работам с использованием методических указаний преподавателя, оформление отчетов и подготовка к защите. Подготовка к тестам. Выполнение курсового проекта **Примерная тематика домашних заданий** 1. Изучение литературы 2. Подготовка к тестированию. 3. 3.Офомление отчета по лабораторной работе. 4. 4.Подготовка к защите лабораторной работы. 5. Разработка и письменное оформление раздела «Введение» 6. Разработка и оформление подраздела «Описание компонентов систем 7. Разработка и оформление подраздела «Выбор и обоснование СЗИ от НСД» **8.** Составить описание методики настройки 9. Разработка и оформление под раздела «Инструменты проверки» 10. Выполнить запуск и регистрацию в системе защиты			184	

1	2	3	4
11. Создать пользователей 12. Реализовать мандатную модель разграничения доступа 13. Реализовать дискреционную модель разграничения доступа 14. Обеспечить замкнутость программной среды 15. Выполнить настройку контроля целостности, регистрации событий, печати штампа. 16. Выполнить настройку гарантированного удаления данных 17. Выполнить и оформить расчёт стоимости работ			
Примерная тематика курсовых проектов 1. Secret Net Studio (версия 8.1) 2. Версия Secret Net 7 (пакет обновлений 7) 3. Secret Net LSP 4. Dallas Lock 8.0-K 5. Dallas Lock 8.0-C 6. Dallas Lock Linux 7. СДЗ Dallas Lock 8. СЗИ ВИ Dallas Lock			
Раздел 2 Применение криптографических средств и методов защиты информации		**194**	
МДК.02.02 Криптографические средства и методы защиты информации		**194**	
Тема 2.1 Основы криптографии	**Содержание**	10	
	1. Основы криптографии. Основные понятия и определения		2
	2. Требования к криптографическим системам		2
	3. Основные уровни безопасности АСОИ		2
	4. Принципы криптографической защиты информации		2
	5. Классификация шифров по разным признакам		2
Тема 2 Традиционные симметричные криптосистемы	**Содержание**	10	
	1. Основные понятия и определения симметричных криптосистем		2
	2. Шифры перестановки		2
	3. Шифры простой замены		2
	4. Шифры сложной замены		2
	5. Шифрование методом гаммирования		2
	Практические работы	10	
	1. Количественная оценка стойкости парольной защиты		

1	2		3	4
	2.	Реализация генератора паролей по заданным требованиям		
	3.	Реализация шифров простой замены при помощи MS Exel		
	4.	Шифр Цезаря на языке программирования		
	5.	Реализация шифра Вижинера		
Тема 2. 3 Современные симметричные криптосистемы	**Содержание**		8	
	1.	Основные понятия современных симметричных криптосистем		2
	2.	Шифр DES		2
	3.	Комбинирование блочных алгоритмов		2
	Практические работы		10	
	1.	Анализ и применение криптосистем		
	2.	Знакомство с принципом шифрования алгоритмом DES		
	3.	Шифр замены по ключу		
	4.	Защита информации с помощью пароля		
	5.	Реализация дискретной модели политики безопасности		
Дифференцированный зачет			**2**	
Тема 2.3 Современные симметричные криптосистемы (продолжение)	**Содержание**		8	
	1.	Алгоритм шифрования IDEA		2
	2.	Отечественный стандарт шифрования данных ГОСТ 28147-89		2
	3.	Блочные и поточные шифры		2
	4.	Криптосистемы с депонированием ключа		2
	Практические работы		4	
	1.	Применение блочных и поточных шифров		
	2.	Применение программы AZRP		
Тема 2.4 Ассиметричные криптосистемы	**Содержание**		4	
	1.	Концепция ассиметричной криптосистемы с открытым ключом		2
	2.	Особенности ассиметричных криптосистем. Однонаправленные функции.		2
Тема 2.5 Алгоритм шифрования RSA	**Содержание**		8	
	1.	Основные действия при шифровании алгоритмом RSA . Безопасность и быстродействие криптосистемы RSA.		2
	2.	Схемы шифрования Полига-Хеллмана и ЭльГамаля.		2
	3.	Комбинированный метод шифрования. Идентификация и проверка подлинности.		2
	4.	Идентификация и аутентификация пользователей.		2
Тема 2.6 Электронно цифровая подпись	**Содержание**		10	
	1.	Электронно цифровая подпись и хеш-функции		2
	2.	Алгоритмы цифровой подписи RSA и Эль-Гамаля		2
	3.	Атаки на алгоритм RSA		2

1	2		3	4
	4.	Цифровые подписи с дополнительными функциональными свойствами. Управление криптографическими ключами		2
	Практические работы		16	
	1.	Знакомство с законом о Цифровой подписи		
	2.	Хеш-функции и их криптографические приложения		
	3.	Знакомство с программой BCalk. Атака на алгоритм шифрования RSA посредством метода Ферма		
	4.	Знакомство с программой PS. Атака на алгоритм шифрования rsa методом повторного шифрования		
	5.	Атака на алгоритм шифрования rsa методом бесключевого чтения		
	6.	Атака на алгоритм шифрования rsa, основанная на китайской теореме об остатках		
	7.	Взлом RSA методом Ферма при неудачном выборе параметров криптосистемы		
	8.	Средства криптографической защиты информации, реализующие основные функции электронной подписи		
Тема 2.7 Электронные платежные системы	**Содержание**		8	
	1.	Принципы функционирования электронных платежных систем		2
	2.	Электронные пластиковые карты		2
	3.	Универсальная электронная платежная система UEPS		2
	4.	Работа с программой PGP. Основные функции PGP		2
	Лабораторные работы		12	
	1.	Классификация и виды электронных платежных систем		
	2.	Знакомство с программой PGP. Создание новых каталогов ключей, генерация ключей		
	3.	Обмен открытыми ключами в программе PGP, импорт ключа		
	4.	Шифрование сообщений в программе PGP. Шифрование сообщения через буфер обмена Windows		
	5.	Шифрование всего файла в программе PGP		
	6.	Расшифровка сообщений через копирование в буфер обмена Windows		
Тема 2.8 Аутентификация. Факторы аутентификации	**Содержание**		10	
	1	Аутентификация с помощью биометрических систем		2
	2	Аутентификация на основе одноразовых паролей		2
	3	Строгая аутентификация, основанная на симметричных алгоритмах		2
	4	Общие сведения о применении криптографии в ПК		2
	5	История появления и развития квантовой криптографии. Применение квантовой криптографии.		2
	Лабораторные работы		6	
	1.	Распределение признаков в биометрии		

1	2		3	4
	2.	Знакомство с программным комплексом SLAnalyzer. Создания своего эталонного шаблона клавиатурного почерка		
	3.	Распознавание пользователя и расчет расстояния от реального пользователя до эталонного с помощью программы SLAnalyzer		
Самостоятельная работа при изучении раздела 2 ПМ 01 Систематическая проработка конспектов занятий, учебной литературы по главам и параграфам, указанным преподавателем. Подготовка к практическим работам с использованием методических указаний преподавателя, оформление отчетов и подготовка к защите. Решение задач на заданную тематику.			58	
Примерная тематика домашних заданий 1. Изучение литературы 1. Оформление отчета по практической работе. 2. Подготовка к защите практической работы. 3. Решение задач «Шифры перестановки 4. Решение задач «Шифры простой замены» 5. Решение задач «Шифры сложной замены» 6. Решение задач «Шифр DES» 7. Решение задач «Комбинирование блочных алгоритмов» 8. Решение задач «Алгоритм шифрования IDEA» 9. Решение задач «Шифрование алгоритмом RSA» 10. Решение задач «Схемы шифрования»				
Раздел 3 Применение метрологии, стандартизации и сертификации на предприятиях			**63**	
МДК.02.03 Метрология, стандартизация и сертификация на предприятиях			**63**	
Введение	**Содержание**		2	
	1.	Содержание и задачи курса. Краткий обзор развития метрологии, стандартизации и сертификации		2
Тема 3.1 Техническое регулирование	**Содержание**		2	
	1.	Техническое регулирование		2
Тема 3.2 Основные сведения о стандартизации	**Содержание**		2	
	1.	Основные сведения о стандартизации		2
Тема 3.3 Принципы и методы стандартизации	**Содержание**		4	
	1.	Принципы и методы стандартизации		2
	2.	Семинар «Основы стандартизации»		2
Тема 3.4 Системы предпочтительных чисел	**Содержание**		2	
	1.	Системы предпочтительных чисел		2

1	2		3	4
	Практические работы		2	
	1.	Ознакомление с рядами предпочтительных чисел		
Тема 3.5 Системы общетехнических стандартов и организационно-методических национальных стандартов	**Содержание**		2	
	1.	Системы общетехнических стандартов и организационно-методических национальных стандартов		2
Тема 3.6 Основные стандарты системы ЕСКД. Правила оформления текстовых документов, виды документации	**Содержание**		2	
	1.	Основные стандарты системы ЕСКД. Правила оформления текстовых документов, виды документации		2
	Практические работы		2	
	1.	Нормоконтроль технической документации		
Тема 3.7 Основные понятия о размерах детали	**Содержание**		1	
	1.	Основные размеры деталей Способы определения и расчеты размеров, годность деталей		2
Тема 3.8 Графическое изображение полей допусков	**Содержание**		1	
	1.	Графическое изображение полей допусков		2
Тема 3.9 Виды посадок	**Содержание**		4	
	1.	Виды посадок		2
	2.	Проверочная работа: «Определение вида соединения»		2
Тема 3.10 Основные понятия сертификации	**Содержание**		2	
	1.	Основные понятия сертификации		2
	Практические работы		2	
	1.	Изучение содержания закона "О техническом регулировании		
Тема 3.11 Показатели качества продукции	**Содержание**		2	
	1.	Показатели качества продукции. Управление качеством продукции		2
Тема 3.12 Управление качеством продукции	**Практические работы**		2	
	1.	Изучение структуры и содержания сертификата		
Тема 3.13 Системы качества по международным стандартам ИСО серии 9000.	**Содержание**		2	
	1.	Системы качества по международным стандартам ИСО серии 9000. Принципы управления качеством		2
Тема 3.14 Принципы управления качеством	**Практические работы**		2	
	1.	Изучение нормативных документов. ГОСТ Р 50936-96 «Защита от несанкционированного доступа к информации»		
Тема 3.15 Основные понятия в области метрологии. **Тема 3.16 Основы обеспечения единства измерений**	**Содержание**		2	
	1.	Основные понятия в области метрологии. Основы обеспечения единства измерений		2
Дифференцированный зачет			**2**	
Самостоятельная работа при изучении раздела 3 ПМ 02 Систематическая проработка конспектов занятий, учебной литературы по главам и параграфам, указанным преподавателем.			**21**	

Подготовка к практическим занятиям с использованием методических указаний преподавателя, оформление отчетов и подготовка к защите. **Примерная тематика домашних заданий** Изучение литературы Подготовка к защите практических работ. Выполнение технических расчетов, оформление технической документации с использованием нормативных документов и государственных стандартов. Подготовка к семинару. Подготовка к проверочным работам, тестам. Составление конспектов на заданную тематику. Составление таблиц и схем на заданную тематику.		
УП.02.01 Учебная практика по работе с базами данных **Виды работ** 1. Проектирование базы данных 2. Проектирование форм для ввода, просмотра и корректировки документов. 3. Тестирование, комплексная отладка базы данных	**72**	
УП.02.02 Учебная практика по выполнению радиомонтажных работ **Виды работ** 1. Обработка и монтаж проводов. 2. Вязка простого жгута. 3. Монтаж односторонних печатных плат. 4. Монтаж двухсторонних печатных плат. 5. Демонтаж печатных плат. 6. Монтаж элементов на печатную плату в соответствии с нормативно-технической документацией.	**72**	
ПП.02.01 Производственная практика (по профилю специальности) **Виды работ** 1. Изучение общей характеристики и структуры предприятия (подразделения) 2. Изучение общей технологической схемы производства и характеристик выпускаемой продукции (услуг). 3. Изучение требований к охране труда на предприятии. 4. Изучение требований к охране труда и экологии на рабочем месте. 5. Участие в применении программно-аппаратные средств обеспечения информационной безопасности в автоматизированных системах. 6. Участие в эксплуатации программно-аппаратных средств обеспечения информационной безопасности, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности. 7. Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации. 8. Решение частных технических задач, возникающих при проведении всех видов плановых и внеплановых контрольных проверок, при аттестации объектов, помещений, программ, алгоритмов. 9. Применение нормативно правовых актов, нормативно-методической документации по обеспечению информационной безопасности программно-аппаратными средствами. 10. Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах. 11. Участие в эксплуатации программно-аппаратных средств обеспечения информационной безопасности, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности.	**396**	

12. Участие в мониторинге эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах. 13. Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации. 14. Решение частных технических задач, возникающих при проведении всех видов плановых и внеплановых контрольных проверок, при аттестации объектов, помещений, программ, алгоритмов. 15. Применение нормативно правовых актов, нормативно-методической документации по обеспечению информационной безопасности программно-аппаратными средствами. 16. Дифференцированный зачет		

Для характеристики уровня освоения учебного материала используются следующие обозначения:
1 – ознакомительный (узнавание ранее изученных объектов, свойств);
2 – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);
3 – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач).

4 УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1 Требования к минимальному материально-техническому обеспечению

Реализация рабочей программы профессионального модуля предполагает наличие лаборатории «Программно-аппаратных средств обеспечения информационной безопасности», «Аппаратных средств вычислительной техники», радиомонтажной мастерской и мастерской «Корпоративная защита от внутренних угроз информационной безопасности».

Оборудование лаборатории «Программно-аппаратных средств обеспечения информационной безопасности»:

- персональные компьютер с аппаратной поддержкой виртуализации и техническими характеристиками не ниже i7\16 Gb \SSD 128\HDD 1 Tb\VGA integrate\ Monitor 23”;
- программное обеспечение VirtualBox, KVM;
- программное обеспечение OpenOffice;
- аппаратное обеспечение ISR G2 (Cisco 2901);
- аппаратное обеспечение Cisco Catalyst WS-2960+24TC-L;
- аппаратное обеспечение Cisco ASA 5505;
- СЗИ от НСД DallasLock, SecretNet;
- АПКШ «Контитнент»;
- специализированное ПО, находящееся в свободном доступе;
- проектор;
- сетевой лазерный принтер для бумаги форматов А3, А4;
- столы и стулья.

Оборудование лаборатории «Аппаратных средств вычислительной техники»:

- персональные компьютер с аппаратной поддержкой виртуализации и техническими характеристиками не ниже i7\16 Gb \SSD 128\HDD 1 Tb\VGA integrate\ Monitor 23”;
- программное обеспечение VirtualBox, KVM ;
- программное обеспечение OpenOffice;
- персональный компьютер и проектор;
- сетевой лазерный принтер для бумаги форматов А3, А4;
- столы и стулья.

Оборудование радиомонтажной мастерской:

– наглядные пособия (стенды, плакаты) по технике безопасности и правилам работы с радиомонтажным оборудованием;
– образцы радиомонтажных работ;
– оборудование радиомонтажника (паяльная станция, набор инструментов для монтажа радиоэлектронной аппаратуры);
– спецодежда для радиомонтажных работ;
– комплектующие (радиоэлементы и печатных платы).

Оборудование мастерской «Корпоративная защита от внутренних угроз информационной безопасности»:

– ПЭВМ в сборе (i7/32Gb MEM/ 256Gb + 1Tb nvme SSD/ Nvidia Qadro 1000 / Intel 4x1Gb/s Lan Card/ 27” Monitor)

– ViPNet Software (Coordinator for Windows 4.x + Client for Windows 4.x + Policy Manager 4.x + VPN HW Router)

– Видео проектор Epson EB-2247U

– Экран для проектора Lumien Master Picture 191x300 Matte White FiberGlass

– Рабочее место в сборе:

- стол (ШхД) 1200x750;
- рама задняя короткая;
- перфопанель – 2;
- набор держателей;
- электроблок на 8 розеток;
- полка приборная длинная;
- светильник светодиодный – 2 шт;
- кронштейн для монитора;
- полка для системного блока;
- стул тканевый с металлической крестовиной;
- металлические колеса для стула;
- набор подлокотников.

4.2 Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. В.Г. Олифер, Н.А. Олифер "Компьютерные сети. Принципы, технологии, протоколы". 5-е изд., – СПб: Питер, 2017.- 992с.

2. Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] — Электрон. дан. — Москва : ДМК Пресс, 2017. — 434 с. — Режим доступа: https://e.lanbook.com/book/93278.

3. Ю.А.Родичев. Нормативная база и стандарты в области информационной безопасности. Учебное пособие - СПб.: Питер, 2017г. – 256стр.

4. Стеганографические и криптографические методы защиты информации: учебное пособие [Электронный ресурс] : учеб. пособие — Электрон. дан. — Уфа : БГПУ имени М. Акмуллы, 2016. — 112 с. — Режим доступа: https://e.lanbook.com/book/90963. — Загл. с экрана.

5. Аверченков, В.И. Криптографические методы защиты информации: учебное пособие [Электронный ресурс] : учеб. пособие / В.И. Аверченков, М.Ю. Рытов, С.А. Шпичак. — Электрон. дан. — Москва : ФЛИНТА, 2017. — 215 с. — Режим доступа: https://e.lanbook.com/book/92914. — Загл. с экрана.

Дополнительные источники:

1. Информационная безопасность Т. Л Партыка, И. И. Попов М: ФОРУМ: ИНФРА-М, 2012
2. Адаменко М.В. Основы классической криптологии:секреты шифров и кодов. ДМК Пресс, 2012 – 256с.:ил.
3. Таненбаум Э., Уэзеролл Д.Компьютерные сети. 5-е изд.. – СПб.: Питер, 2018. – 960 с.

Интернет-ресурсы:

1. cisco.com
2. netacad.com

4.3 Общие требования к организации образовательного процесса

Занятия проводятся спаренными уроками продолжительностью один академический час, общая продолжительность спаренного урока - 2 академических часа (1,5 астрономических часа). Образовательный процесс включает в себя проведение лекционных, комбинированных, практических занятий и лабораторных работ, чередующихся друг с другом.

Учебная практика по выполнению радиомонтажных работ реализуется концентрированно в радиомонтажной мастерской и лабораториях колледжа. Каждый обучающийся должен быть обеспечен индивидуальным рабочим местом.

Реализация рабочей программы модуля должна обеспечиваться учебно методической документацией, доступом каждого обучающегося к базам данных и библиотечным фондам. Во время самостоятельной подготовки обучающиеся должны быть обеспечены доступом к сети Интернет.

Должны быть предусмотрены консультации в объеме не менее 0,5 часа в неделю по каждому МДК. Формы проведения консультаций: групповые, индивидуальные, письменные, устные.

Освоению данного модуля должно предшествовать изучение следующих дисциплин:

- ОП.01 Основы информационной безопасности;
-ОП.02 Технические средства информатизации;
- ОП.03 Организационно-правовое обеспечение информационной безопасности;
- ОП.04 Сети и системы передачи информации;
-ОП.05 Основы алгоритмизации и программирования
- ОП.07Операционные системы;
-ОП.08 Базы данных;
- ОП.14 Архитектура ЭВМ и вычислительных систем

4.4 Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических (инженерно-педагогических) кадров, обеспечивающих обучение по междисциплинарным курсам:

- наличие высшего профессионального образования, соответствующего профилю профессионального модуля «Программно-аппаратные средства обеспечения информационной безопасности» и «Криптографические средства и методы защиты информации»;

- опыт деятельности в организациях соответствующей профессиональной сферы, эти преподаватели должны проходить стажировку в профильных организациях не реже 1 раза в 3 года.

Требования к квалификации педагогических кадров, осуществляющих руководство практикой:

- дипломированные специалисты по профилю профессионального модуля;
- мастера производственного обучения;
- преподаватели междисциплинарных курсов.

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ВИДА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)

Результаты (освоенные профессиональные компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
Применять программно-аппаратные средства обеспечения информационной безопасности в автоматизированных системах.	Правильно применяет программно-аппаратные средства обеспечения информационной безопасности в автоматизированных системах.	Наблюдение за выполнение и защита лабораторных работ по МДК 02.01 Защита курсового проекта. Выполнение работ и дифференцированный зачет по учебной практике УП02.02. Дифференцированный зачет. Выполнение работ и отчет по производственной практике по профилю специальности. Возможна сдача ДЭ по компетенции «Корпоративная защита от внутренних угроз информационной безопасности» по КОД 1.1
Участвовать в эксплуатации программно-аппаратных средств обеспечения информационной безопасности, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности.	Правильно проверяет техническое состояние программно-аппаратных средств обеспечения информационной безопасности. Правильно проводит техническое обслуживание и текущий ремонт, устраняет отказы и восстанавливает работоспособность программно-аппаратных средств обеспечения информационной безопасности.	Наблюдение за выполнение и защита лабораторных работ по МДК 02.01 Защита курсового проекта. Дифференцированный зачет. Выполнение работ и дифференцированный зачет по учебной практике УП02.02. Выполнение работ и отчет по производственной практике по профилю специальности. Возможна сдача ДЭ по компетенции «Корпоративная защита от внутренних угроз информационной безопасности» по КОД 1.1

Участвовать в мониторинге эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах.	Правильно проводит мониторинг эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности	Наблюдение за выполнение и защита лабораторных работ по МДК 02.01, МДК02.02. Выполнение работ и дифференцированный зачет по учебной практике УП02.01. Защита курсового проекта. Выполнение работ и отчет по производственной практике по профилю специальности Возможна сдача ДЭ по компетенции «Корпоративная защита от внутренних угроз информационной безопасности» по КОД 1.1
Участвовать в обеспечении учета, обработки, хранения и передачи конфиденциальной информации.	Правильно выполняет учет, обработку, хранение и передачу конфиденциальной информации.	Наблюдение за выполнение и защита лабораторных работ по МДК 02.01, МДК02.02. Выполнение работ и дифференцированный зачет по учебной практике УП02.01. Защита курсового проекта. Выполнение работ и отчет по производственной практике по профилю специальности. Возможна сдача ДЭ по компетенции «Корпоративная защита от внутренних угроз информационной безопасности» по КОД 1.1
Решать частные технические задачи, возникающие при проведении всех видов плановых и внеплановых контрольных проверок, при аттестации объектов, помещений, программ, алгоритмов.	Правильно проводит плановые и внеплановые контрольные проверки при аттестации объектов, помещений, программ, алгоритмов. .	Наблюдение за выполнение и защита лабораторных работ по МДК 02.01, МДК02.02. Выполнение работ и дифференцированный зачет по учебной практике УП02.01. Защита курсового проекта. Выполнение работ и отчет по производственной практике по профилю специальности

		Возможна сдача ДЭ по компетенции «Корпоративная защита от внутренних угроз информационной безопасности» по КОД 1.1
Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности программно-аппаратными средствами.	Правильно применяет нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности программно-аппаратными средствами.	Наблюдение за выполнение и защита лабораторных работ по МДК 02.01, МДК02.02, МДК02.03. Выполнение работ и дифференцированный зачет по учебной практике УП02.01. Защита курсового проекта. Выполнение работ и отчет по производственной практике по профилю специальности Возможна сдача ДЭ по компетенции «Корпоративная защита от внутренних угроз информационной безопасности» по КОД 1.1

Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся не только сформированность профессиональных компетенций, но и развитие общих компетенций и обеспечивающих их умений.

Результаты (освоенные общие компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности.	Демонстрация интереса к будущей профессии.	*Наблюдение за выполнением и защита лабораторных работ, выполнение тестирования, выполнение курсового проекта, выполнение работ по учебным практикам и производственной практики по профилю специальности.*
Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество	Правильная организация собственной деятельности, правильный выбор и применение методов и способов решения профессиональных задач для программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах и криптографических средств и методы защиты информации; - правильность оценки эффективности и качества разработки.	
Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.	Правильная работа автоматизированных систем после решения проблем в нестандартных и стандартных ситуаций, в области применения программно – аппаратных средств обеспечения ИБ в АС.	
Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.	Правильная работа автоматизированной системы согласно поставленной задаче.	
Использовать информационно-коммуникационные технологии в профессиональной деятельности	Использование актуальных технологий в профессиональной деятельности.	
Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.	Взаимодействие с преподавателями, мастерами, обучающимися в ходе учебного процесса и производственной практики	
Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий	Ответственность за выполнение заданий, полученных группой студентов	
Самостоятельно определять задачи профессионального и личностного развития,	Организация самостоятельных занятий при изучении профессионального модуля;	

заниматься самообразованием, осознанно планировать повышение квалификации,	Самоанализ и коррекция результатов собственной работы.	
Ориентироваться в условиях частой смены технологий в профессиональной деятельности	Проявление интереса к инновациям в области применения программно – аппаратных средств обеспечения ИБ в АС.	*Посещение выставок, выполнение практических и лабораторных работ.*
Формулировать задачи логического характера и применять средства математической логики для их решения.	Использование математической логики, решение задач логического характера	*Наблюдение за выполнением лабораторных работ, курсового проекта, учебных и производственной практик*
Владеть основными методами и средствами разработки программного обеспечения	Использование методов и средств разработки программного обеспечения	*Наблюдение за выполнением лабораторных работ, учебной практики УП.02.01*
Производить инсталляцию и настройку автоматизированных информационных систем, выполнять в автоматизированных информационных системах регламентные работы по обновлению, техническому сопровождению и восстановлению при отказах.	Правильное выполнение инсталляции и настройки АИС, регламентных работ в АИС	*Наблюдение за выполнением и защита лабораторных работ, курсового проекта, учебных и производственной практик*