

Департамент образования Ярославской области
Государственное профессиональное образовательное учреждение
Ярославской области Переславский колледж им. А. Невского

**РАБОЧАЯ ПРОГРАММА
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

**ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ
ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ**

для специальности: 10.02.05 Обеспечение информационной безопасности
автоматизированных систем

Рабочая программа профессионального модуля разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Организация-разработчик: ГПОУ ЯО Переславский колледж им. А. Невского

Разработчики: Агаркова О.В., Малыгина С.Ю., Сукин И.А. - преподаватели
ГПОУ ЯО Переславский колледж им. А. Невского

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	4
2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	7
3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	23
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	29

**1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ
ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ**

1.1. Цель и планируемые результаты освоения профессионального модуля

1.1.1. В результате изучения профессионального модуля студент должен освоить вид деятельности *Защита информации в автоматизированных системах программными и программно-аппаратными средствами* и соответствующие ему профессиональные компетенции:

Код	Наименование видов деятельности и профессиональных компетенций
ВД 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.

1.1.2. Общие компетенции

Код	Наименование видов деятельности и профессиональных компетенций
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания

	необходимого уровня физической подготовленности.
ОК 9.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.

1.1.3. В результате освоения профессионального модуля студент должен:

Иметь практический опыт	<ul style="list-style-type: none"> – 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	<ul style="list-style-type: none"> – 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	<ul style="list-style-type: none"> – 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.

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего 828 часов, из них: на освоение МДК – 520 часов, в том числе, на промежуточную аттестацию по МДК – 12 часов; на самостоятельную работу по МДК - 44 часа, на подготовку к экзамену по профессиональному модулю - 4 часа; на учебную и производственную практики – 252 часа; на экзамен по модулю – 8 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

Коды профессиональных общих компетенций	Наименования разделов профессионального модуля	Объем образовательной программы, час.	Объем профессионального модуля, час.					
			Обучение по МДК, в час.			Практики		Самостоятельная работа
			всего, часов	в том числе		учебная практика, часов	производственная практика, часов	
лабораторных и практических занятий	курсовая работа (проект), часов							
ПК 2.1 – ПК 2.6 ОК 1-ОК 10	Раздел 1 модуля. Применение программных и программно-аппаратных средств защиты информации	480	334	148	32	108		38
ПК 2.4 ОК 1-ОК 10	Раздел 2 модуля. Применение криптографических средств защиты информации	228	186	98	–	36		6
ПК 2.1 – ПК 2.6 ОК 1-ОК 10	Производственная практика по ПМ.02	108					108	
ПК 2.1 – ПК 2.6 ОК 1-ОК 10	Экзамен по профессиональному модулю	12	8	–	–	–	–	4
	Всего:	828	528	246	32	144	108	48

МДК.02.01. Программные и программно-аппаратные средства защиты информации		372
Раздел 1. Основные принципы программной и программно-аппаратной защиты информации		78
Тема 1.1. Предмет и задачи программно-аппаратной защиты информации	Содержание	6
	Предмет и задачи программно-аппаратной защиты информации	2
	Основные понятия программно-аппаратной защиты информации	2
	Классификация методов и средств программно-аппаратной защиты информации	2
Тема 1.2. Стандарты безопасности	Содержание	6
	Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.	2
	Профили защиты программных и программно-аппаратных средств (межсетевых экранов, средств контроля съемных машинных носителей информации, средств доверенной загрузки, средств антивирусной защиты)	2
	Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.	2
	Практические занятия	6
	Обзор нормативных правовых актов, нормативных методических документов по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.	2
	Работа с содержанием нормативных правовых актов.	2
	Обзор стандартов. Работа с содержанием стандартов	2
Тема 1.3. Защищенная автоматизированная система	Содержание	10
	Автоматизация процесса обработки информации. Понятие автоматизированной системы.	2
	Особенности автоматизированных систем в защищенном исполнении. Основные виды АС в защищенном исполнении.	2
	Методы создания безопасных систем Методология проектирования гарантированно защищенных КС	2
	Дискреционные модели	2
	Мандатные модели	2
	Практические занятия	26

	Создание виртуальных машин и установка ОС	2
	Разворачивание домена на сервере	2
	Учет, обработка, хранение и передача информации в АИС	2
	Ограничение доступа на вход в систему.	2
	Идентификация и аутентификация пользователей	2
	Разграничение доступа.	2
	Регистрация событий (аудит).	2
	Контроль целостности данных	2
	Уничтожение остаточной информации.	2
	Управление политикой безопасности. Шаблоны безопасности	2
	Криптографическая защита. Обзор программ шифрования данных	2
	Шифрование файлов и дисков	2
	Управление политикой безопасности. Шаблоны безопасности	2
Тема 1.4.	Содержание	6
Дестабилизирующее воздействие на объекты защиты	Источники дестабилизирующего воздействия на объекты защиты	2
	Способы воздействия на информацию	2
	Причины и условия дестабилизирующего воздействия на информацию	2
	Практические занятия	4
	Распределение каналов в соответствии с источниками воздействия на информацию	2
	Анализ причин и условий дестабилизирующего воздействия на информацию	2
Тема 1.5. Принципы программно-аппаратной защиты информации от несанкционированного доступа	Содержание	8
	Понятие несанкционированного доступа к информации	2
	Основные подходы к защите информации от НСД	
	Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам	2
	Доступ к данным со стороны процесса	2
	Особенности защиты данных от изменения. Шифрование.	2
	Практические занятия	6

	Организация доступа к файлам	4
	Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД	2
Раздел 2. Защита автономных автоматизированных систем		102
Тема 2.1. Основы защиты автономных автоматизированных систем	Содержание	8
	Работа автономной АС в защищенном режиме	2
	Алгоритм загрузки ОС. Штатные средства замыкания среды. Расширение BIOS как средство замыкания программной среды	2
	Системы типа Электронный замок. ЭЗ с проверкой целостности программной среды. Понятие АМДЗ (доверенная загрузка)	2
	Применение закладок, направленных на снижение эффективности средств, замыкающих среду.	2
	Практические занятия	6
	Расширение BIOS	2
	Применение закладок	2
	Применение системы типа Электронный замок	2
Тема 2.2. Защита программ от изучения	Содержание	8
	Изучение и обратное проектирование ПО	2
	Способы изучения ПО: статическое и динамическое изучение	2
	Задачи защиты от изучения и способы их решения	2
	Защита от отладки. Защита от дизассемблирования Защита от трассировки по прерываниям.	2
Тема 2.3. Вредоносное программное обеспечение	Содержание	10
	Вредоносное программное обеспечение как особый вид разрушающих воздействий. Классификация вредоносного программного обеспечения. Схема заражения. Средства нейтрализации вредоносного ПО. Профилактика заражения	2
	Поиск следов активности вредоносного ПО. Реестр Windows. Основные ветки, содержащие информацию о вредоносном ПО. Другие объекты, содержащие информацию о вредоносном ПО, файлы prefetch.	2
	Бот-нет. Принцип функционирования. Методы обнаружения	2
	Классификация антивирусных средств. Сигнатурный и эвристический анализ. Защита от вирусов в "ручном режиме"	2

	Основные концепции построения систем антивирусной защиты на предприятии	2
	Практические занятия	8
	Имитация вирусной атаки и поиск следов активности вредоносного ПО	2
	Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО	2
	Нарушение дискреционной политики безопасности программой «Троянский конь»	4
Тема 2.4. Защита программ и данных от несанкционированного копирования	Содержание	8
	Несанкционированное копирование программ как тип НСД	2
	Юридические аспекты несанкционированного копирования программ. Общее понятие защиты от копирования.	2
	Привязка ПО к аппаратному окружению и носителям.	2
	Защитные механизмы в современном программном обеспечении на примере MS Office	2
	Практические занятия	8
	Защита информации от несанкционированного копирования с использованием специализированных программных средств	2
	Управление сертификатами в операционной системе Windows	4
	Защитные механизмы в приложениях (на примере MSWord, MSExcel, MSPowerPoint)	2
Тема 2.5. Защита информации на машинных носителях	Содержание	12
	Проблема защиты отчуждаемых компонентов ПЭВМ. Методы защиты информации на отчуждаемых носителях.	2
	Шифрование.	2
	Средства восстановления остаточной информации. Создание посекторных образов НЖМД.	2
	Применение средств восстановления остаточной информации в судебных криминалистических экспертизах и при расследовании инцидентов. Нормативная база, документирование результатов	4
	Безвозвратное удаление данных. Принципы и алгоритмы.	2
	Практические занятия	8
	Применение средства восстановления остаточной информации на примере Foremost или аналога	2
	Применение специализированного программного средства для восстановления удаленных файлов	2
Применение программ для безвозвратного удаления данных	2	

	Применение программ для шифрования данных на съемных носителях	2
Тема 2.6. Аппаратные средства идентификации и аутентификации пользователей	Содержание	4
	Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ	2
	Устройства Touch Memory	2
	Практические занятия	2
	Двухфакторная аутентификация	2
Тема 2.7. Системы обнаружения атак и вторжений	Содержание	14
	СОВ и СОА, отличия в функциях. Основные архитектуры СОВ	2
	Использование сетевых sniffеров в качестве СОВ	2
	Аппаратный компонент СОВ	2
	Программный компонент СОВ	2
	Модели системы обнаружения вторжений.	2
	Классификация систем обнаружения вторжений.	2
	Обнаружение сигнатур. Обнаружение аномалий. Другие методы обнаружения вторжений.	2
	Практические занятия	6
	Моделирование проведения атаки.	2
	Изучение инструментальных средств обнаружения вторжений.	2
	Работа с анализаторами трафика	2
Раздел 3. Защита информации в локальных сетях		18
Тема 3.1. Основы построения защищенных сетей	Содержание	4
	Сети, работающие по технологии коммутации пакетов. Штатные средства защиты информации стека протоколов TCP/IP.	2
	Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения.	2
	Практические занятия	2
	Изучение протоколов сетевого и транспортного уровней стека TCP/IP	2
Тема 3.2. Средства	Содержание	8

организации VPN	Виртуальная частная сеть. Функции, назначение, принцип построению Криптографические и некриптографические средства организации VPN	2
	Устройства, образующие VPN. Криptomаршрутизатор и криптофильтр.	2
	Криптороутер. Принципы, архитектура, модель нарушителя, достоинства и недостатки	2
	Криптофильтр. Принципы, архитектура, модель нарушителя, достоинства и недостатки	2
	Практические занятия	4
	Развертывание VPN	4
Раздел 4. Защита информации в сетях общего доступа		22
Тема 4.1. Обеспечение безопасности межсетевого взаимодействия	Содержание	12
	Методы защиты информации при работе в сетях общего доступа.	2
	Межсетевые экраны типа firewall. Достоинства, недостатки, реализуемые политики безопасности. Основные типы firewall. Симметричные и несимметричные firewall.	2
	Уровень 1. Пакетные фильтры	2
	Уровень 2. Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне.	2
	Уровень 3. Проху-сервера прикладного уровня	2
	Однохостовые и мультихостовые firewall. Основные типы архитектур мультихостовых firewall. Требования к каждому хосту исходя из архитектуры и выполняемых функций. Требования по сертификации межсетевых экранов	2
	Практические работы	10
	Изучение и сравнение архитектур Dual Homed Host, Bastion Host, Perimetr.	2
	Изучение различных способов закрытия "опасных" портов	2
	Настройка межсетевого экрана	2
	Настройка протокола IPSec	4
Раздел 5. Защита информации в базах данных		18
Тема 5.1. Защита информации в базах данных	Содержание	10
	Основные типы угроз. Модель нарушителя	2
	Средства идентификации и аутентификации. Управление доступом	2
	Средства контроля целостности информации в базах данных	2

	Средства аудита и контроля безопасности. Критерии защищенности баз данных	2
	Применение криптографических средств защиты информации в базах данных	2
	Практические занятия	8
	Изучение механизмов защиты СУБД MS Access	2
	Изучение механизмов защиты СУБД по выбору	2
	Изучение механизмов идентификации и аутентификации, управления доступом	2
	Изучение штатных средств защиты СУБД MSSQL Server	2
Раздел 6. Мониторинг систем защиты		58
Тема 6.1. Мониторинг систем защиты	Содержание	10
	Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации	2
	Особенности фиксации событий, построенных на разных принципах: сети с коммутацией соединений, сеть с коммутацией пакетов, TCP/IP, X.25	2
	Классификация отслеживаемых событий.	2
	Особенности построения систем мониторинга. Источники информации для мониторинга: сетевые мониторы, статистические характеристики трафика через МЭ, проверка ресурсов общего пользования. Классификация сетевых мониторов	2
	Системы управления событиями информационной безопасности (SIEM). Обзор SIEM-систем на мировом и российском рынке.	2
	Практические занятия	16
	Изучение и сравнительный анализ распространенных сетевых мониторов на примере RealSecure, SNORT, NFR или других аналогов	4
	Фиксация событий, построенных на разных принципах: сети с коммутацией соединений	4
	Фиксация событий, построенных на разных принципах: сеть с коммутацией пакетов, TCP/IP, X.25	4
	Проведение аудита ЛВС сетевым сканером	4
Тема 6.2. Изучение мер защиты информации в	Содержание	4
	Изучение требований о защите информации, не составляющей государственную тайну.	2
	Изучение методических документов ФСТЭК по применению мер защиты.	2

информационных системах	Практические занятия	8
	Выбор мер защиты информации для их реализации в информационной системе.	4
	Выбор соответствующих программных и программно-аппаратных средств и рекомендаций по их настройке.	4
Тема 6.3. Изучение современных программно-аппаратных комплексов.	Практические работы	20
	Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов	4
	Установка и настройка программных средств оценки защищенности и аудита информационной безопасности, изучение функций и настройка режимов работы на примере MaxPatrol 8 или других аналогов	4
	Изучение типовых решений для построения VPN на примере VipNet или других аналогов	4
	Изучение современных систем антивирусной защиты на примере корпоративных решений KasperskyLab или других аналогов	4
	Изучение функционала и областей применения DLP систем на примере InfoWatchTrafficMonitor или других аналогов	4
Курсовая работа		32
Примерная тематика курсовых работ		
<ol style="list-style-type: none"> 1. Оценка эффективности существующих программных и программно-аппаратных средств защиты информации с применением специализированных инструментов и методов (индивидуальное задание) 2. Обзор и анализ современных программно-аппаратных средств защиты информации (индивидуальное задание) 3. Выбор оптимального средства защиты информации исходя из методических рекомендаций ФСТЭК и имеющихся исходных данных (индивидуальное задание) 4. Применение программно-аппаратных средств защиты информации от различных типов угроз на предприятии (индивидуальное задание) 5. Проблема защиты информации в облачных хранилищах данных и ЦОДах 6. Защита сред виртуализации 		
Самостоятельная работа		38
Работа над курсовым проектом (работой): планирование выполнения курсового проекта (работы), определение задач работы, изучение литературных источников, проведение предпроектного исследования.		32

Подготовка к промежуточной аттестации		6
Промежуточная аттестация по МДК.02.01 в форме экзамена		6
Учебная практика по разделу 1 модуля		108
Виды работ:		
<ul style="list-style-type: none"> – Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах – Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности – Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности – Составление документации по учету, обработке, хранению и передаче конфиденциальной информации – Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации – Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов. – Устранение замечаний по результатам проверки – Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов. – Применение математических методов для оценки качества и выбора наилучшего программного средства 		
МДК.02.02. Криптографические средства защиты информации		192
Введение	Содержание	2
	Предмет и задачи криптографии. История криптографии. Основные термины	
Раздел 1. Математические основы защиты информации		48
Тема 1.1.	Содержание	30
Математические основы криптографии	Основы теории сложности и асимптотического анализа алгоритмов.	
	Элементы теории множеств. Абстрактная алгебра, группы, кольца, поля.	
	Делимость чисел. Признаки делимости. Простые и составные числа.	
	Основная теорема арифметики. Наибольший общий делитель. Взаимно простые числа. Алгоритм Евклида для нахождения НОД.	
	Отношения сравнимости. Свойства сравнений. Модулярная арифметика.	

	Классы. Полная и приведенная система вычетов.	
	Функция Эйлера. Теорема Ферма-Эйлера.	
	Алгоритм быстрого возведения в степень по модулю. Китайская теорема об остатках.	
	Конечные поля. Расширения полей, комплексные числа.	
	Квадратичные вычеты.	
	Арифметические операции над большими числами. Быстрое возведение в степень. Поиск образующего элемента циклической группы.	
	Проверка чисел на простоту. Метод Ферма. Метод Миллера-Рабина. Существование полиномиальных алгоритмов проверки на простоту. Метод Агравала-Каяла-Саксены.	
	Разложение числа на множители. Числа Мерсенна. Алгоритмы факторизации. Факторизация Ферма. Метод Полларда.	
	Алгоритмы дискретного логарифмирования. Метод Полларда.	
	Эллиптические кривые и их приложения в криптографии. Метод Ленстры.	
	Практические занятия	18
	Применение алгоритма быстрого возведения в степень по модулю.	
	Выполнение арифметических операций над большими числами.	
	Работа с алгоритмами факторизации.	
	Применение метода Агравала-Каяла-Саксены.	
	Применение метода Полларда.	
	Применение метода Ленстры.	
	Применение алгоритма Евклида для нахождения НОД чисел и многочленов над конечными полями.	
	Проверка чисел на простоту. Разложение на множители чисел специального вида.	
	Решение других задач с элементами теории чисел.	
	Раздел 2. Классическая криптография	36
Тема 2.1. Методы криптографического защиты информации	Содержание	8
	Классификация основных методов криптографической защиты. Методы симметричного шифрования	
	Шифры замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр	
	Матричные шифры, рюкзачные шифры.	

	Современные методы симметричного шифрования. DES.	
	Практические занятия	6
	Применение классических шифров замены	
	Применение классических шифров перестановки	
	Применение DES.	
Тема 2.2. Криптоанализ	Содержание	6
	Основные методы криптоанализа. Криптографические атаки.	
	Криптографическая стойкость. Абсолютно стойкие криптосистемы. Принципы Керкгоффа	
	Перспективные направления криптоанализа, квантовый криптоанализ.	
	Практические занятия	8
	Криптоанализ шифра простой замены методом анализа частотности символов	
	Криптоанализ классических шифров методом полного перебора ключей	
	Криптоанализ шифров Виженера и Плейфера.	
Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел	Содержание учебного материала	4
	Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии	
	Методы получения псевдослучайных последовательностей.	
	Практические занятия	4
	Применение метода шифрования RC4	
	Применение методов генерации ПСЧ	
Раздел 3. Современная криптография		94
Тема 3.1. Кодирование информации. Компьютеризация шифрования.	Содержание учебного материала	10
	Теория кодирования. Символьное кодирование. Смысловое кодирование.	
	Представление информации в двоичном коде.	
	Компьютеризация шифрования. Аппаратное и программное шифрование	
	Стандартизация программно-аппаратных криптографических систем и средств.	
	Изучение современных программных и аппаратных криптографических средств	
	Практические занятия	8

	Кодирование информации	
	Программная реализация классических шифров	
	Изучение реализации классических шифров замены и перестановки в программе СrupTool или аналоге.	
Тема 3.2. Симметричные системы шифрования	Содержание учебного материала	6
	Общие сведения. Структурная схема симметричных криптографических систем	
	Отечественные алгоритмы Магма и Кузнечик. Стандарты ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015.	
	Симметричные алгоритмы DES, AES, ГОСТ 28147-89	
	Практические занятия	6
	Изучение программной реализации современных симметричных шифров	
Тема 3.3. Асимметричные системы шифрования	Содержание учебного материала	6
	Криптосистемы с открытым ключом. Необратимость систем. Структурная схема шифрования с открытым ключом.	
	Алгоритм RSA.	
	Элементы теории чисел в криптографии с открытым ключом.	
	Практические занятия	6
	Применение различных асимметричных алгоритмов. Изучение программной реализации асимметричного алгоритма RSA	
Тема 3.4. Аутентификация данных. Электронная подпись	Содержание учебного материала	6
	Аутентификация данных. Общие понятия. ЭП. MAC. Однонаправленные хеш-функции. Алгоритмы цифровой подписи	
	Практические занятия	8
	Применение различных функций хеширования, анализ особенностей хешей	
	Применение криптографических атак на хеш-функции.	
	Изучение программно-аппаратных средств, реализующих основные функции ЭП	
Тема 3.5. Алгоритмы обмена ключей и протоколы	Содержание учебного материала	6
	Алгоритмы распределения ключей с применением симметричных и асимметричных схем Протоколы аутентификации. Взаимная аутентификация. Односторонняя аутентификация	

аутентификации	Практические занятия	6
	Применение протокола Диффи-Хеллмана для обмена ключами шифрования.	
	Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.	
Тема 3.6. Криптозащита информации в сетях передачи данных	Содержание учебного материала	4
	Абонентское шифрование. Пакетное шифрование. Защита центра генерации ключей. Криптомаршрутизатор. Пакетный фильтр	
	Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протокола WPA.	
Тема 3.7. Защита информации в электронных платежных системах	Содержание учебного материала	4
	Принципы функционирования электронных платежных систем. Электронные пластиковые карты. Персональный идентификационный номер. Криптовалюты.	
	Применение криптографических протоколов для обеспечения безопасности электронной коммерции.	
	Практические занятия	8
	Применение криптографических протоколов для обеспечения безопасности электронной коммерции.	
	Применение аутентификации по одноразовым паролям.	
	Реализация алгоритмов создания одноразовых паролей.	
Тема 3.8. Компьютерная стеганография	Содержание учебного материала	6
	Скрытая передача информации в компьютерных системах. Проблема аутентификации мультимедийной информации. Защита авторских прав.	
	Методы компьютерной стеганографии.	
	Цифровые водяные знаки. Алгоритмы встраивания ЦВЗ	
	Практические занятия	4
	Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ	
	Реализация простейших стеганографических алгоритмов	
Самостоятельная работа обучающихся: подготовка к промежуточной аттестации		6
Промежуточная аттестация по МДК.02.02 в форме экзамена		6

Учебная практика раздела 2 модуля Виды работ: – Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи	36
Производственная практика по ПМ.02 Виды работ – Анализ принципов построения систем информационной защиты производственных подразделений. – Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы. – Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности; – Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении – Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации – Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики.	108
Подготовка к промежуточной аттестации	4
Экзамен по профессиональному модулю	8
Всего:	828

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Для реализации программы профессионального модуля должны быть предусмотрены следующие специальные помещения:

Реализация программы предполагает наличие учебных кабинетов – лекционные аудитории с мультимедийным оборудованием; лаборатории «Программных и программно-аппаратных средств обеспечения информационной безопасности».

Оборудование учебного кабинета и рабочих мест кабинета – лекционная аудитория: посадочных мест - 30, рабочее место преподавателя, проектор, персональный компьютер, комплект презентаций.

Оборудование лаборатории «Программных и программно-аппаратных средств обеспечения информационной безопасности» и рабочих мест лаборатории:

- рабочие места студентов, оборудованные персональными компьютерами;
- лабораторные учебные макеты;
- рабочее место преподавателя;
- учебно-методическое обеспечение модуля;
- интерактивная доска, комплект презентаций;
- антивирусные программные комплексы;
- программно-аппаратные средства защиты информации от НСД, блокировки доступа и нарушения целостности;
- программные и программно-аппаратные средства обнаружения атак (вторжений), поиска уязвимостей;
- средства уничтожения остаточной информации в запоминающих устройствах;
- программные средства криптографической защиты информации.

3.2. Информационное обеспечение обучения

3.2.1 Основные печатные источники:

1. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии: учеб. Пособие. – М.: Горячая линия – Телеком, 2017.- 175 с.

2. Душкин А.В., Барсуков О.М., Кравцов Е.В., Славнов К.В. Программно-аппаратные средства обеспечения информационной безопасности: учеб. Пособие. – М.: Горячая линия – Телеком, 2018.- 248 с.

3. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 1. Правовое обеспечение информационной безопасности: учеб. Пособие. – М.: МИЭТ, 2017. – 184 с.

4. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2016. – 172 с.

5. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2017. – 336с

6. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие - Москва: МИФИ, 2012.- 400 с.

Рекомендовано УМО «Ядерные физика и технологии» в качестве учебного пособия для студентов высших учебных заведений.

7. Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В. Основы криптографии (учебное пособие). - М.: Гелиос АРВ, 2015. – гриф Министерства образования РФ по группе специальностей в области информационной безопасности

8. Мельников В.П., Клейменов С.А., Петраков А.М.: Информационная безопасность и защита информации М.: Академия, - 336 с. – 2017

9. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд-во: ДМК Пресс, - 2016

10. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2016. – 416 с.

3.2.2. Дополнительные печатные источники:

1. Погорелов Б.А., Сачков В.Н. (ред.). Словарь криптографических терминов. - М.: МЦНМО, 2006. Словарь криптографических терминов. Под ред. Б.А. Погорелова и В.Н. Сачкова. – М.: МЦНМО, 2006 г

2. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

3. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

4. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

5. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

6. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».

7. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

8. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

9. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

10. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.

11. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.

12. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

13. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.

14. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.
15. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.
16. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
17. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.
18. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.
19. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.
20. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недеklarированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.
21. Приказ ФАПСИ при Президенте Российской Федерации от 13 июня 2001 г. № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».
22. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».
23. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий
24. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий
25. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер
26. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети
27. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью

28. ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель
29. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
30. ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности
31. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"
32. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"
33. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
34. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.
35. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.
36. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.
37. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
38. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005.
39. ГОСТ Р 50543-93 Конструкции базовые несущие. Средства вычислительной техники. Требования по обеспечению защиты информации и электромагнитной совместимости методом экранирования. Госстандарт России, 1993.
40. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.
41. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.
42. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.
43. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013.
44. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК

России 14 февраля 2008 г.

45. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

46. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

47. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

48. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

49. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

50. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

51. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

в) программное обеспечение: специализированное программное обеспечение для проверки защищенности помещений от утечки информации по акустическому и виброакустическому каналам, специальных исследований средств вычислительной техники;

г) базы данных, информационно-справочные и поисковые системы: www.fstec.ru; www.gost.ru/wps/portal/tk362.

3.2.3. Периодические издания:

1. Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей;

2. Защита информации. Инсайд: Информационно-методический журнал

3. Информационная безопасность регионов: Научно-практический журнал

4. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности.. URL: <http://cyberrus.com/>

5. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: <http://bit.mephi.ru/>

3.2.4. Электронные источники:

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru

2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru

3. Образовательные порталы по различным направлениям образования и тематике <http://depobr.gov35.ru/>

4. справочно-правовая система «Консультант Плюс» www.consultant.ru

5. Справочно-правовая система «Гарант» » www.garant.ru
6. Федеральный портал «Российское образование www.edu.ru
7. Федеральный правовой портал «Юридическая Россия» <http://www.law.edu.ru/>
8. Российский биометрический портал www.biometrics.ru
9. Федеральный портал «Информационно- коммуникационные технологии в образовании» [http\\:www.ict.edu.ru](http://www.ict.edu.ru)
10. Сайт Научной электронной библиотеки www.elibrary.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	Критерии оценки	Методы оценки
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	Демонстрировать умения и практические навыки в установке и настройке отдельных программных, программно-аппаратных средств защиты информации	тестирование, экзамен, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	Демонстрировать знания и умения в обеспечении защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	тестирование, экзамен, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.	Выполнение перечня работ по тестированию функций отдельных программных и программно-аппаратных средств защиты информации	тестирование, экзамен, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач,

		оценка процесса и результатов выполнения видов работ на практике
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	Проявлять знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа	тестирование, экзамен, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.	Демонстрация алгоритма проведения работ по уничтожению информации и носителей информации с использованием программных и программно-аппаратных средств	тестирование, экзамен, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
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	Проявлять знания и умения в защите автоматизированных (информационных) систем с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	тестирование, экзамен, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике

компьютерных атак.		
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	<ul style="list-style-type: none"> – обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач 	<p>Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы</p> <p>Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам</p> <p>Экзамен квалификационный</p>
ОП 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	<ul style="list-style-type: none"> - использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач 	
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	<ul style="list-style-type: none"> - демонстрация ответственности за принятые решения - обоснованность самоанализа и коррекция результатов собственной работы; 	
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	<ul style="list-style-type: none"> - взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных) 	
ОК 05. Осуществлять устную и письменную коммуникацию на	<ul style="list-style-type: none"> - грамотность устной и письменной речи, - ясность формулирования 	

государственном языке с учетом особенностей социального и культурного контекста.	и изложения мыслей	
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.	- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик,	
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; - знание и использование ресурсосберегающих технологий в области телекоммуникаций	
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик;	
ОК 09. Использовать информационные технологии в профессиональной деятельности.	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	
---	--	--