ЧАСТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«СТАВРОПОЛЬСКИЙ МНОГОПРОФИЛЬНЫЙ КОЛЛЕДЖ»

ПРОГРАММА
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

для обучающихся специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

2023

Аннотация

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

Рабочая программа учебной дисциплины разработана в соответствии с Федеральным государственным образовательным стандартом среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем утверждённым приказом Минобрнауки России от 09.12.2016 г. №1553 и в соответствии с учебным планом СмК специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утверждённым директором колледжа Кандауровой Н.В. на 2023 - 2024 учебный год.

Организация-разработчик: Частное образовательное учреждение профессионального образования "Ставропольский многопрофильный колледж".

Разработчики:

1. Хвалько Леонид Александрович

Данные не найдены (Нет информации о согласовании)

Рассмотрено на заседании методического объединения ого цикла Укрупненных групп специальностей 09.00.00 «Информатика и вычислительная техника»; 10.00.00 «Информационная безопасность»

Протокол №6 от 26.05.2023

Председатель МО Хвалько Леонид Александрович

Рекомендовано к использованию в учебном процессе методическим советом

Протокол №7 от 26.05.2023

Председатель МС Шляхова Наталья Ивановна

1. ПАСПОРТ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ

1.1. Область применения программы

Рабочая программа профессионального модуля является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности **10.02.05 Обеспечение информационной безопасности автоматизированных систем в части освоения основного вида деятельности (ВД) ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами и соответствующие общие, профессиональные компетенции и личностные результаты.**

1.1.1. Перечень общих компетенций

Код	Наименование общих компетенций
ОК 02.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 03.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 09.	Использовать информационные технологии в профессиональной деятельности.
ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 04.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 06.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.
ОК 07.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 08.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.

1.1.2. Перечень профессиональных компетенций

Код	Наименование профессиональных компетенций
ВД	
ПК 2.4.	Осуществлять обработку, хранение и передачу информации ограниченного доступа.
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 2.6.	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.
ПК 2.5.	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.

1.1.3. Перечень личностных результатов

Код	Наименование личностных результатов
ЛР 13	Демонстрирующий готовность и способность вести диалог с другими людьми, достигать в нем взаимопонимания, находить общие цели и сотрудничать для их достижения в профессиональной деятельности
ЛР 17	Умеющий рационально использовать время, информацию и материальные ресурсы, соблюдать порядок на рабочем месте, осуществлять коллективную работу в Компании
ЛР 18	Способный адаптироваться к новой ситуации и применять новые подходы к решению возникающих проблем
ЛР 23	Вовлеченный в работу добровольческих (волонтерских) объединений по организации акций, посвященных памятным событиям в истории России. Принимающий принципы добровольчества (волонтерства) в сфере оказания помощи ветеранам Великой Отечественной войны и боевых действий, благоустройства памятных мест и воинских захоронений
ЛР 27	Развивающий и углубляющий знания об истории, культуре России и Ставропольского края
ЛР 1	Осознающий себя гражданином и защитником великой страны
ЛР 22	Выработавший принципы экологически целесообразного поведения, бережного отношения к своей жизни, жизни других людей, природы, планеты в целом
ЛР 3	Соблюдающий нормы правопорядка, следующий идеалам гражданского общества, обеспечения безопасности, прав и свобод граждан России. Лояльный к установкам и проявлениям представителей субкультур, отличающий их от групп с деструктивным и девиантным поведением. Демонстрирующий неприятие и предупреждающий социально опасное поведение окружающих
ЛР 16	Выработавший умения и навыки трудовой деятельности, проявляющий основы трудовой культуры по отношению к коллегам, контрагентам и клиентам Компании

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 освоить следующие результаты:

Умение:

- устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;;
- диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;;
- 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;
- Применять математический аппарат для выполнения криптографических преобразований;;
- Проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;;

Знание:

- типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;;
- методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;;
- Особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;;
- Типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.;
- особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;;
- основные понятия криптографии и типовых криптографических методов и средств защиты информации;;

1.3. Рекомендуемое количество часов на освоение программы профессионального модуля

Всего - 356 час(-а, -ов), в том числе:

максимальной учебной нагрузки обучающегося - 356 час(-а, -ов), включая:

- обязательной аудиторной учебной нагрузки обучающегося - 356 час(-а, -ов)

2. СОДЕРЖАНИЕ ОБУЧЕНИЯ ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихс, курсовая работа (проект) (если предусмотрены)	Объём в часах	Уровень освоения	Коды компетенций и личностных результатов, формированию которых способствует элемент программы
	МДК.02.01 Программные и программно-аппаратные средства защиты информации	210		
Тема 1 Предмет и задачи программно-аппаратной защиты информации	Содержание учебного материала			ЛР 13, ЛР 18, ЛР 17, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 **Лекционные занятия №1** Предмет и задачи программно-аппаратной защиты информации	2	1	
	2 **Практические занятия №1** Знакомство с файловой системой	2	2	
Тема 2 Основные понятия программно-аппаратной защиты информации	Содержание учебного материала			ЛР 18, ЛР 17, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6., ЛР 13
	1 **Лекционные занятия №2** Основные понятия программно-аппаратной защиты информации	2	1	
	2 **Практические занятия №2** Работа с файлами	2	2	
Тема 3 Классификация методов и средств программно-аппаратной защиты информации	Содержание учебного материала			ЛР 13, ЛР 18, ЛР 17, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 **Лекционные занятия №3** Классификация методов и средств программно-аппаратной защиты информации	2	1	
	2 **Практические занятия №3** Работа с каталогами	2	2	
Тема 4 Классификация угроз безопасности операционной системы	Содержание учебного материала			ЛР 13, ЛР 18, ЛР 17, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 **Лекционные занятия №4** Классификация угроз безопасности операционной системы	2	1	
	2 **Практические занятия №4** Работа с файлами и каталогами	2	2	
Тема 5 Основные средства и методы защиты информации в операционной системе. Часть 1.	Содержание учебного материала			ЛР 13, ЛР 18, ЛР 17, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 **Лекционные занятия №5** Основные средства и методы защиты информации в операционной системе. Часть 1.	2	1	
	2 **Практические занятия №5** Командные файлы и программирование	2	2	
Тема 6 Основные средства и методы защиты информации в операционной системе. Часть 2	Содержание учебного материала			ЛР 13, ЛР 18, ЛР 17, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 **Лекционные занятия №6** Основные средства и методы защиты информации в операционной системе. Часть 2	2	1	
	2 **Практические занятия №6** Командные файлы	2	2	

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихс, курсовая работа (проект) (если предусмотрены)		Объём в часах	Уровень освоения	Коды компетенций и личностных результатов, формированию которых способствует элемент программы
Тема 7 Разграничение доступа к объектам операционной системы. Часть 1	Содержание учебного материала				ЛР 13, ЛР 18, ЛР 17, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1	**Лекционные занятия №7** Разграничение доступа к объектам операционной системы. Часть 1	2	1	
	2	**Практические занятия №7** Использование командных файлов Часть 1	2	2	
Тема 8 Разграничение доступа к объектам операционной системы. Часть 2	Содержание учебного материала				ЛР 13, ЛР 18, ЛР 17, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1	**Лекционные занятия №8** Разграничение доступа к объектам операционной системы. Часть 2	2	1	
	2	**Практические занятия №8** Использование командных файлов Часть 2	2	2	
Тема 9 Стандарты защищенности операционных систем. Часть 1	Содержание учебного материала				ЛР 18, ЛР 13, ЛР 17, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1	**Лекционные занятия №9** Стандарты защищенности операционных систем. Часть 1	2	1	
Тема 10 Стандарты защищенности операционных систем. Часть 2	Содержание учебного материала				ЛР 13, ЛР 18, ЛР 17, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1	**Лекционные занятия №10** Стандарты защищенности операционных систем. Часть 2	2	1	
Тема 11 Защита информации в операционной системе Windows.	Содержание учебного материала				ЛР 17, ЛР 13, ЛР 18, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1	**Лекционные занятия №11** Защита информации в операционной системе Windows.	2	1	
Тема 12 Защита информации в операционной системе Linux	Содержание учебного материала				ЛР 13, ЛР 17, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6., ЛР 18
	1	**Лекционные занятия №12** Защита информации в операционной системе Linux	2	1	
Тема 13 Защита информации в базах данных. Часть 1	Содержание учебного материала				ЛР 13, ЛР 18, ЛР 17, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1	**Лекционные занятия №13** Защита информации в базах данных. Часть 1	2	1	
Тема 14 Защита информации в базах данных. Часть 2.	Содержание учебного материала				ЛР 18, ЛР 13, ЛР 17, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1	**Лекционные занятия №14** Защита информации в базах данных. Часть 2.	2	1	

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихс, курсовая работа (проект) (если предусмотрены)		Объём в часах	Уровень освоения	Коды компетенций и личностных результатов, формированию которых способствует элемент программы
Тема 15 Многоуровневая модель безопасности баз данных. Многозначность.	Содержание учебного материала				ЛР 18, ЛР 13, ЛР 17, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1	**Лекционные занятия №15** Многоуровневая модель безопасности баз данных. Многозначность.	2	1	
Тема 16 Защита информации от разрушающих программных воздействий. Понятие разрушающего программного воздействия	Содержание учебного материала				ЛР 18, ЛР 13, ЛР 17, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1	**Лекционные занятия №16** Защита информации от разрушающих программных воздействий. Понятие разрушающего программного воздействия	2	1	
Тема 17 Программа с потенциально опасными последствиями.	Содержание учебного материала				ЛР 13, ЛР 18, ЛР 17, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1	**Лекционные занятия №17** Программа с потенциально опасными последствиями.	2	1	
	2	**Практические занятия №9** Разные команды Windows	2	2	
	3	**Курсовая работа** Курсовая работа	2	2	
	4	**Курсовая работа** Курсовая работа	2	2	
Тема 18 Модели взаимодействия прикладной программы и программной закладки	Содержание учебного материала				ЛР 13, ЛР 17, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6., ЛР 18
	1	**Лекционные занятия №18** Модели взаимодействия прикладной программы и программной закладки	2	1	
	2	**Практические занятия №10** Элементы программирования в BASH. Файлы сценариев Часть 1	2	2	
	3	**Курсовая работа** Курсовая работа	2	2	
	4	**Курсовая работа** Курсовая работа	2	2	
Тема 19 Методы перехвата и навязывания информации	Содержание учебного материала				ЛР 18, ЛР 13, ЛР 17, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1	**Лекционные занятия №19** Методы перехвата и навязывания информации	2	1	
	2	**Практические занятия №11** Элементы программирования в BASH. Файлы сценариев Часть 2	2	2	
	3	**Курсовая работа** Курсовая работа	2	2	
	4	**Курсовая работа** Курсовая работа	2	2	
Тема 20 Классификация и методы внедрения программных закладок	Содержание учебного материала				ЛР 18, ЛР 17, ЛР 13, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1	**Лекционные занятия №20** Классификация и методы внедрения программных закладок	2	1	
	2	**Практические занятия №12** Виды информации и основные методы ее защиты.	2	2	
	3	**Курсовая работа** Курсовая работа	2	2	
	4	**Курсовая работа** Курсовая работа	2	2	
Тема 21 Компьютерные вирусы как особый класс разрушающих программных воздействий. Часть 1	Содержание учебного материала				ЛР 18, ЛР 13, ЛР 17, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1	**Лекционные занятия №21** Компьютерные вирусы как особый класс разрушающих программных воздействий. Часть 1	2	1	
	2	**Практические занятия №13** Виды угроз информационной безопасности Российской Федерации.	2	2	
	3	**Курсовая работа** Курсовая работа	2	2	
	4	**Курсовая работа** Курсовая работа	2	2	

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихс, курсовая работа (проект) (если предусмотрены)		Объём в часах	Уровень освоения	Коды компетенций и личностных результатов, формированию которых способствует элемент программы
Тема 22 Компьютерные вирусы как особый класс разрушающих программных воздействий. Часть 2	Содержание учебного материала				ЛР 13, ЛР 18, ЛР 17, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1	**Лекционные занятия №22** Компьютерные вирусы как особый класс разрушающих программных воздействий. Часть 2	2	1	
	2	**Практические занятия №14** Источники угроз информационной безопасности Российской Федерации.	2	2	
	3	**Курсовая работа** Курсовая работа	2	2	
	4	**Курсовая работа** Курсовая работа	2	2	
Тема 23 Понятие изолированной программной среды. Часть 1.	Содержание учебного материала				ЛР 13, ЛР 17, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6., ЛР 18
	1	**Лекционные занятия №23** Понятие изолированной программной среды. Часть 1.	2	1	
	2	**Практические занятия №15** Анализ информационной инфраструктуры государства.	2	2	
	3	**Курсовая работа** Курсовая работа	2	2	
	4	**Курсовая работа** Курсовая работа	2	2	
Тема 24 Понятие изолированной программной среды. Часть 2.	Содержание учебного материала				ЛР 13, ЛР 18, ЛР 17, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1	**Лекционные занятия №24** Понятие изолированной программной среды. Часть 2.	2	1	
	2	**Практические занятия №16** Исследование атаки переполнения буфера как примера нарушения конфиденциальности, целостности и доступности информации	2	2	
	3	**Курсовая работа** Курсовая работа	2	2	
Тема 25 Методы защиты информации при работе в сетях общего доступа.	Содержание учебного материала				ЛР 13, ОК 08., ЛР 18, ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6., ЛР 17, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07.
	1	**Лекционные занятия №25** 1. Методы защиты информации при работе в сетях общего доступа.	2	1	
	2	**Лабораторные занятия №1** 1. Защита информации от несанкционированного копирования с использованием специализированных программных средств.	2	2	
	3	**Практические занятия №17** 1. Моделирование проведения атаки. Изучение инструментальных средств обнаружения вторжений	2	2	
	4	**Практическая подготовка №1** 1. Изучение и сравнение архитектур Dual Homed Host, Bastion Host, Perimetr.	4	2	
Тема 26 Межсетевые экраны типа firewall.	Содержание учебного материала				ЛР 18, ЛР 13, ЛР 17, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1	**Лекционные занятия №26** 2. Межсетевые экраны типа firewall.	2	1	
	2	**Лабораторные занятия №2** 2. Защитные механизмы в приложениях (на примере MSWord, MSExcel, MSPowerPoint) Часть 1.	2	2	
	3	**Практические занятия №18** 2. Развертывание VPN.	2	2	
	4	**Практическая подготовка №2** 2. Изучение и сравнительный анализ распространенных сетевых мониторов на примере RealSecure, SNORT, NFR или других аналогов	4	2	

Наименование разделов ПМ, МДК и тем		Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихс, курсовая работа (проект) (если предусмотрены)	Объём в часах	Уровень освоения	Коды компетенций и личностных результатов, формированию которых способствует элемент программы
Тема 27 Достоинства, недостатки, реализуемые политики безопасности	Содержание учебного материала				ЛР 13, ЛР 18, ЛР 17, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1	**Лекционные занятия №27** 3. Достоинства, недостатки, реализуемые политики безопасности	2	1	
	2	**Лабораторные занятия №3** 3. Защитные механизмы в приложениях (на примере MSWord, MSExcel, MSPowerPoint) Часть 2.	2	2	
	3	**Практические занятия №19** 3. Изучение различных способов закрытия "опасных" портов.	2	2	
	4	**Практическая подготовка №3** 3. Выбор соответствующих программных и программно-аппаратных средств и рекомендаций по их настройке.	4	2	
Тема 28 Основные типы firewall. Симметричные и несимметричные firewall.	Содержание учебного материала				ЛР 18, ЛР 13, ЛР 17, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1	**Лекционные занятия №28** 4. Основные типы firewall. 5. Симметричные и несимметричные firewall.	2	1	
	2	**Лабораторные занятия №4** 4. Применение средства восстановления остаточной информации на примере Foremost или аналога	2	2	
	3	**Практические занятия №20** 4. Изучение механизмов защиты СУБД MS Access	2	2	
	4	**Практическая подготовка №4** 4. Установка и настройка программных средств оценки защищенности и аудита информационной безопасности.	4	2	
Тема 29 Пакетные фильтры.	Содержание учебного материала				ЛР 13, ЛР 18, ЛР 17, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1	**Лекционные занятия №29** 6. Пакетные фильтры.	2	1	
	2	**Лабораторные занятия №5** 5. Применение специализированного программно средства для восстановления удаленных файлов	2	2	
	3	**Практические занятия №21** 5. Изучение штатных средств защиты СУБД MSSQL Server	2	2	
	4	**Практическая подготовка №5** 5. Изучение функций и настройка режимов работы на примере MaxPatrol 8 или других аналогов	4	2	
Тема 30 Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне.	Содержание учебного материала				ЛР 13, ЛР 18, ЛР 17, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1	**Лекционные занятия №30** 7. Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне.	2	1	
	2	**Лабораторные занятия №6** 6. Применение программ для безвозвратного удаления данных	2	2	
	3	**Практические занятия №22** 6. Проведение аудита ЛВС сетевым сканером.	2	2	
	4	**Практическая подготовка №6** 6. Изучение типовых решений для построения VPN на примере VipNet или других аналогов	4	2	
Тема 31 Proxy-сервера прикладного уровня.	Содержание учебного материала				ЛР 18, ЛР 13, ЛР 17, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1	**Лекционные занятия №31** 8.Proxy-сервера прикладного уровня.	2	1	
	2	**Лабораторные занятия №7** 7. Применение программ для шифрования данных на съемных носителях.	2	2	
	3	**Практические занятия №23** 7. Выбор мер защиты информации для их реализации в информационной системе.	2	2	
	4	**Практическая подготовка №7** 7. Изучение современных систем антивирусной защиты на примере корпоративных решений KasperskyLab или других аналогов.	4	2	

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихс, курсовая работа (проект) (если предусмотрены)	Объём в часах	Уровень освоения	Коды компетенций и личностных результатов, формированию которых способствует элемент программы
Тема 32 Однохостовые и мультихостовые firewall.	Содержание учебного материала			ЛР 18, ЛР 13, ЛР 17, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 **Лекционные занятия №32** 8. Однохостовые и мультихостовые firewall.	2	1	
	2 **Практические занятия №24** 8.Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов.	2	2	
	3 **Практическая подготовка №8** 8. Изучение функционала и областей применения DLP систем на примере InfoWatchTrafficMonitor или других аналогов.	4	2	
Тема 33 Основные типы архитектур мультихостовых firewall.	Содержание учебного материала			ЛР 13, ЛР 18, ЛР 17, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 **Лекционные занятия №33** 9. Основные типы архитектур мультихостовых firewall.	2	1	
Тема 34 Требования к каждому хосту исходя из архитектуры и выполняемых функций	Содержание учебного материала			ЛР 13, ЛР 18, ЛР 17, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 **Лекционные занятия №34** 10.Требования к каждому хосту исходя из архитектуры и выполняемых функций	2	1	
Тема 35 Требования по сертификации межсетевых экранов.	Содержание учебного материала			ЛР 13, ЛР 17, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6., ЛР 18
	1 **Лекционные занятия №35** 11. Требования по сертификации межсетевых экранов.	2	1	
Тема 36 Основные типы угроз. Модель нарушителя.	Содержание учебного материала			ЛР 13, ЛР 18, ЛР 17, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 **Лекционные занятия №36** 12. Основные типы угроз. Модель нарушителя.	2	1	
Тема 37 Средства идентификации и аутентификации. Управление доступом.	Содержание учебного материала			ЛР 18, ЛР 17, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6., ЛР 13
	1 **Лекционные занятия №37** 13. Средства идентификации и аутентификации. Управление доступом.	2	1	
Тема 38 Средства контроля целостности информации в базах данных.	Содержание учебного материала			ЛР 18, ЛР 17, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6., ЛР 13
	1 **Лекционные занятия №38** 14. Средства контроля целостности информации в базах данных.	2	1	
Тема 39 Средства аудита и контроля безопасности. Критерии защищенности баз данных	Содержание учебного материала			ЛР 18, ЛР 13, ЛР 17, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 **Лекционные занятия №39** 15. Средства аудита и контроля безопасности. Критерии защищенности баз данных	2	1	

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихс, курсовая работа (проект) (если предусмотрены)	Объём в часах	Уровень освоения	Коды компетенций и личностных результатов, формированию которых способствует элемент программы
Тема 40 Применение криптографических средств защиты информации в базах данных.	Содержание учебного материала			ЛР 13, ЛР 18, ЛР 17, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 **Лекционные занятия №40** 16. Применение криптографических средств защиты информации в базах данных.	2	1	
	2 **Часы на контроль** Промежуточная аттестация	6	2	
Курсовая работа		**30**	30	ОК 02., ОК 03., ОК 05., ОК 09., ОК 01., ОК 04., ОК 06., ОК 07., ОК 08., ОК 10., ПК 2.4., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.6., ПК 2.5., ЛР 13, ЛР 17, ЛР 18, ЛР 23, ЛР 27
Форма(-ы) контроля - 4 семестр, Курсовая работа; 5 семестр, Экзамен				
Всего по МДК.02.01 Программные и программно-аппаратные средства защиты информации		210		
МДК.02.02 Криптографические средства защиты информации		146		

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихс, курсовая работа (проект) (если предусмотрены)		Объём в часах	Уровень освоения	Коды компетенций и личностных результатов, формированию которых способствует элемент программы
Тема 1 Лекции	Содержание учебного материала				ОК 02., ОК 05., ОК 01., ОК 06., ОК 08., ЛР 1, ЛР 3, ЛР 16, ПК 2.3., ЛР 22, ПК 2.1., ПК 2.6.
	1	**Лекционные занятия №1** Криптографические средства с древнего времени	2	1	
	2	**Лекционные занятия №2** Шифр Гая Юлия Цезаря	2	1	
	3	**Лекционные занятия №3** Шифр перестановки Шифр перестановки «сцитала»	2	1	
	4	**Лекционные занятия №4** Диск Энея. Квадрат Полибия	2	1	
	5	**Лекционные занятия №5** Шифр Чейза. Тюремный шифр	2	1	
	6	**Лекционные занятия №6** Шифр Виженера. Шифр Фальконера. Шифр Кеплера и Галилея	2	1	
	7	**Лекционные занятия №7** Основные понятия криптографии	2	1	
	8	**Лекционные занятия №8** Термины и определения в области информационной безопасности	2	1	
	9	**Лекционные занятия №9** Правовое регулирование применения СКЗИ и ЭП в корпоративных информационных системах.	2	1	
	10	**Лекционные занятия №10** Специальные нормативные и методические документы ФСБ России по использованию шифровальных (криптографических) средств	2	1	
	11	**Лекционные занятия №11** Функции, используемые в криптографических системах	2	1	
	12	**Лекционные занятия №12** Однонаправленные функции	2	1	
	13	**Лекционные занятия №13** Имитостойкость	2	1	
	14	**Лекционные занятия №14** Криптографическая стойкость	2	1	
	15	**Лекционные занятия №15** Практическая криптографическая стойкость	2	1	
	16	**Лекционные занятия №16** Классификация поточных шифров	2	1	
	17	**Лекционные занятия №17** Регистр сдвига с линейной обратной связью	2	1	
	18	**Лекционные занятия №18** Линейная сложность	2	1	
	19	**Лекционные занятия №19** Методы и способы криптографической защиты информации.	2	1	
	20	**Лекционные занятия №20** Инфраструктура открытых ключей (ИОК/PKI).	2	1	
	21	**Лекционные занятия №21** Криптосистема	2	1	
	22	**Лекционные занятия №22** Криптосистема	2	1	
	23	**Лекционные занятия №23** Криптосистема	2	1	
	24	**Лекционные занятия №24** Сертификаты	2	1	
	25	**Лекционные занятия №25** Сети и сетевой доступ	2	1	
	26	**Лекционные занятия №26** Способы предотвращения удаленных атак на информационные системы	2	1	
	27	**Лекционные занятия №27** Защита от атак	2	1	
	28	**Лекционные занятия №28** Методы криптографии	2	1	
	29	**Лекционные занятия №29** Межсетевой экран	2	1	
	30	**Лекционные занятия №30** Фильтрация на сетевом уровне	2	1	
	31	**Лекционные занятия №31** Фильтрация на прикладном уровне	2	1	
	32	**Лекционные занятия №32** Обзор сертифицированных шифровальных (криптографических) средств защиты информации. Методика оценки и выбора СКЗИ.	2	1	

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихс, курсовая работа (проект) (если предусмотрены)		Объём в часах	Уровень освоения	Коды компетенций и личностных результатов, формированию которых способствует элемент программы
Тема 2 Практические занятия	Содержание учебного материала				ОК 08., ОК 02., ПК 2.6., ЛР 1, ЛР 3, ОК 05., ОК 01., ОК 06., ЛР 16, ЛР 22, ПК 2.3., ПК 2.1.
	1	**Практические занятия №1** Введение в криптографическую защиту информации	2	2	
	2	**Практические занятия №2** Основы криптографической защиты информации	2	2	
	3	**Практические занятия №3** потоковое шифрование данных	2	2	
	4	**Практические занятия №4** исследование методов полиалфавитной подстановки	2	2	
	5	**Практические занятия №5** разработка и исследование криптоалгоритма на основе использования скремблера	2	2	
	6	**Практические занятия №6** алгоритм блочного шифрования данных гост 28147-89	2	2	
	7	**Практические занятия №7** симметричное и асимметричное шифрование данных средствами криптографического пакета openssl. Часть 1.	2	2	
	8	**Практические занятия №8** симметричное и асимметричное шифрование данных средствами криптографического пакета openssl. Часть 2.	2	2	
	9	**Практические занятия №9** шифрование сообщений с помощью шифров замены криптографическими функциями excel	2	2	
	10	**Практические занятия №10** исследование работы простейших алгоритмов шифрования в среде программирования delphi	2	2	
	11	**Практические занятия №11** исследование функций гаммирования на языке программирования java	2	2	

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихс, курсовая работа (проект) (если предусмотрены)		Объём в часах	Уровень освоения	Коды компетенций и личностных результатов, формированию которых способствует элемент программы
Тема 3 Практическая подготовка	Содержание учебного материала				ОК 02., ОК 05., ОК 01., ОК 08., ОК 06., ПК 2.3., ПК 2.1., ЛР 16, ЛР 22, ПК 2.6., ЛР 1, ЛР 3
	1	**Практическая подготовка №1** шифрование методом перестановки	4	2	
	2	**Практическая подготовка №2** Исследование гаммирования при шифровании	4	2	
	3	**Практическая подготовка №3** симметричное шифрование данных с использованием криптографических интерфейсов microsoft cryptoapi и cryptography api: next generation	4	2	
	4	**Практическая подготовка №4** создание криптографических сообщений с использованием интерфейса microsoft cryptoapi и цифровых сертификатов x.509	4	2	
	5	**Практическая подготовка №5** исследование возможностей блочного шифрования на языке программирования java	4	2	
	6	**Практическая подготовка №6** исследование возможностей поточного шифрования на языке программирования java	2	2	
	7	**Практическая подготовка №7** программная реализация шифров на языке программирования java	2	2	
	8	**Практическая подготовка №8** исследование блочного алгоритма шифрования des	2	2	
	9	**Практическая подготовка №9** исследование алгоритма шифрования rsa в ms	2	2	
	10	**Практическая подготовка №10** средства обеспечения безопасности ос семейства windows	2	2	
	11	**Практическая подготовка №11** асимметричная криптография и электронная цифровая подпись на примере системы gnupg	2	2	
	12	**Практическая подготовка №12** аутентификация пользователей web-систем средствами технологии php	2	2	
	13	**Практическая подготовка №13** защита информации с помощью пароля	2	2	
	14	**Практическая подготовка №14** Удостоверяющие центры на основе службы сертификации в операционной системе Windows 2003 Server	2	2	
	15	**Практическая подготовка №15** Защита программ от несанкционированного использования с помощью USB-ключей и программного обеспечения производителя	2	2	
	16	**Практическая подготовка №16** Защита программ от несанкционированного использования с помощью USB-ключей и средств разработчика	2	2	
Тема 4 Промежуточная аттестация	Содержание учебного материала				ЛР 22, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6., ЛР 1, ЛР 3, ЛР 16
	1	**Часы на контроль** Промежуточная аттестация	18	2	
Форма(-ы) контроля - 4 семестр, Экзамен					
Всего по МДК.02.02 Криптографические средства защиты информации			146		
Всего по ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами			**356**		

Для характеристики уровня освоения учебного материала используются следующие обозначения:

1 - ознакомительный (ознакомление с ранее изученными объектами, свойствами);

2 - репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);
3 - продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач).

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Требования к минимальному материально-техническому обеспечению профессионального модуля ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

Реализация МДК.02.01 Программные и программно-аппаратные средства защиты информации предполагает наличие помещений:

Кабинет информационных систем в профессиональной деятельности
Кабинет информатики и математики
Кабинет компьютерного дизайна
Лаборатория информационных технологий в профессиональной деятельности
Лаборатория информационных технологий
Лаборатория компьютерного дизайна
Лаборатория разработки веб-приложений
Студия инженерной и компьютерной графики
Студия разработки дизайна веб-приложений
Кабинет для самостоятельной работы

- Системный блок (9 шт.)
- Монитор (9 шт.)
- Мышь компьютерная (9 шт.)
- Стенды (1 шт.)
- Клавиатура (9 шт.)
- Плакаты (34 шт.)

Лаборатория сетей и систем передачи информации
Лаборатория электроники и схемотехники
Лаборатория программных и программно-аппаратных средств защиты информации
Лаборатория технических средств защиты информации
Полигон вычислительной техники
Полигон учебных баз практик
Методический кабинет
Кабинет для самостоятельной работы

- Монитор (9 шт.)
- Мышь компьютерная (9 шт.)
- Системный блок (9 шт.)
- Стенды (3 шт.)

- Клавиатура (9 шт.)

Компьютерный класс
Кабинет информатики
Лаборатория технологии разработки баз данных
Лаборатория системного и прикладного программирования
Лаборатория информационно-коммуникационных систем
Лаборатория управления проектной деятельностью
Лаборатория вычислительной техники, архитектуры персонального компьютера и периферийных устройств
Лаборатория программного обеспечения и сопровождения компьютерных систем
Лаборатория программирования и баз данных
Лаборатория организации и принципов построения информационных систем
Лаборатория информационных ресурсов

- Клавиатура (16 шт.)
- Матрешка – Z (набор – конструктор) (5 шт.)
- Robobuilder RQ – HUNO (Многофункциональный робот-андроид) (1 шт.)
- Монитор (16 шт.)
- Мышь компьютерная (16 шт.)
- Плакаты (32 шт.)
- Системный блок (16 шт.)
- Стенды (4 шт.)

Реализация МДК.02.02 Криптографические средства защиты информации предполагает наличие помещений:

Лаборатория сетей и систем передачи информации
Лаборатория электроники и схемотехники
Лаборатория программных и программно-аппаратных средств защиты информации
Лаборатория технических средств защиты информации
Полигон вычислительной техники
Полигон учебных баз практик
Методический кабинет
Кабинет для самостоятельной работы

- Монитор (9 шт.)
- Мышь компьютерная (9 шт.)
- Системный блок (9 шт.)

- Стенды (3 шт.)
- Клавиатура (9 шт.)

Компьютерный класс
Кабинет информатики
Лаборатория технологии разработки баз данных
Лаборатория системного и прикладного программирования
Лаборатория информационно-коммуникационных систем
Лаборатория управления проектной деятельностью
Лаборатория вычислительной техники, архитектуры персонального компьютера и периферийных устройств
Лаборатория программного обеспечения и сопровождения компьютерных систем
Лаборатория программирования и баз данных
Лаборатория организации и принципов построения информационных систем
Лаборатория информационных ресурсов

- Клавиатура (16 шт.)
- Матрешка – Z (набор – конструктор) (5 шт.)
- Robobuilder RQ – HUNO (Многофункциональный робот-андроид) (1 шт.)
- Монитор (16 шт.)
- Мышь компьютерная (16 шт.)
- Плакаты (32 шт.)
- Системный блок (16 шт.)
- Стенды (4 шт.)

3.2. Учебно-методическое и информационное обеспечение профессионального модуля

Перечень рекомендуемых учебных изданий и дополнительной литературы для **МДК.02.01 Программные и программно-аппаратные средства защиты информации**:

Основная литература:

1. 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
2. Информационная безопасность : учебник / В.П. Мельников, А.И. Куприянов. — Москва : КноРус, 2018. Режим доступа https://www.book.ru/book/924214

Дополнительная литература:

1. Куль, Т.П. Операционные системы : учебное пособие / Т.П. Куль. - Минск : РИПО, 2019. - 312 с. - ISBN 978-985-503-940-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1056304
2. Информатика, автоматизированные информационные технологии и системы : учебник / В.А. Гвоздева. — М. : ИД «ФОРУМ» : ИНФРА-М, 2019. — 542 с. — (Среднее профессиональное образование). - Режим доступа: http://znanium.com/catalog/product/999615

Информационные справочно-правовые системы и ресурсы:

1. Электронно-библиотечная система Znanium.com
2. Электронно- библиотечная система BOOK.RU

Перечень рекомендуемых учебных изданий и дополнительной литературы для **МДК.02.02 Криптографические средства защиты информации**:

Основная литература:

1. 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
2. Информационная безопасность : учебник / В.П. Мельников, А.И. Куприянов. — Москва : КноРус, 2018. Режим доступа https://www.book.ru/book/924214

Дополнительная литература:

1. Информационная безопасность: Учебное пособие / Партыка Т. Л., Попов И. И. - 5-е изд., перераб. и доп. - М.: Форум, НИЦ ИНФРА-М, 2016. - 432 с.: 60x90 1/16. - (Профессиональное образование) (Переплёт) ISBN 978-5-91134-627-0 - Режим доступа: http://znanium.com/catalog/product/516806
2. Информатика, автоматизированные информационные технологии и системы : учебник / В.А. Гвоздева. — М. : ИД «ФОРУМ» : ИНФРА-М, 2019. — 542 с. — (Среднее профессиональное образование). - Режим доступа: http://znanium.com/catalog/product/999615

Информационные справочно-правовые системы и ресурсы:

1. Электронно-библиотечная система Znanium.com

2. Электронно- библиотечная система BOOK.RU

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

4.1. Таблица соответствия компетенций показателям оценки результата

Результаты (освоенные профессиональные и общие компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
ОК		Данные не найдены (основные показатели оценки результата)
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	Данные не найдены (формы и методы контроля и оценки)	
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	Данные не найдены (формы и методы контроля и оценки)	
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	Данные не найдены (формы и методы контроля и оценки)	
ОК 09. Использовать информационные технологии в профессиональной деятельности.	Данные не найдены (формы и методы контроля и оценки)	
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	Данные не найдены (формы и методы контроля и оценки)	
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	Данные не найдены (формы и методы контроля и оценки)	
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.	Данные не найдены (формы и методы контроля и оценки)	
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	Данные не найдены (формы и методы контроля и оценки)	
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.	Данные не найдены (формы и методы контроля и оценки)	
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.	Данные не найдены (формы и методы контроля и оценки)	
ПК		Данные не найдены (основные показатели оценки результата)
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	Данные не найдены (формы и методы контроля и оценки)	
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	Данные не найдены (формы и методы контроля и оценки)	
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	Данные не найдены (формы и методы контроля и оценки)	
ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.	Данные не найдены (формы и методы контроля и оценки)	
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.	Данные не найдены (формы и методы контроля и оценки)	
ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.	Данные не найдены (формы и методы контроля и оценки)	

4.2. Образовательные результаты освоения образовательной программы профессионального модуля, подлежащие проверке

Наименование образовательного результата	Показатели оценки результата	Формы и методы контроля и оценки результата
Умение		
устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;	Уметь устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;	Тестирование
диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;	Уметь диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;	Тестирование
устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;	Уметь устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;	Тестирование
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	Уметь 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	Тестирование
Применять математический аппарат для выполнения криптографических преобразований;	Уметь применять математический аппарат для выполнения криптографических преобразований;	Тестирование
Проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;	Уметь проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;	Тестирование
Знание		
типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;	Знать типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;	Коллоквиум
методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;	Знать методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;	Коллоквиум
Особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;	Знать особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;	Коллоквиум
Типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.	Знать типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.	Коллоквиум
особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;	Знать особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;	Коллоквиум
основные понятия криптографии и типовых криптографических методов и средств защиты информации;	Знать основные понятия криптографии и типовых криптографических методов и средств защиты информации;	Коллоквиум

4.3. Матрица соответствия контрольно-оценочных средств образовательным результатам профессионального модуля

Результаты обучения	Коды компетенций	Фонды оценочных средств
Умение		

Результаты обучения	Коды компетенций	Фонды оценочных средств
устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;	ЛР 13, ЛР 17, ЛР 18, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6. (МДК.02.01);	Вопросы на экзамен №25-32 (МДК.02.01);
диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;	ЛР 13, ЛР 17, ЛР 18, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6. (МДК.02.01);	Вопросы на экзамен №41-50 (МДК.02.01);
устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;	ЛР 13, ЛР 17, ЛР 18, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6. (МДК.02.01);	Вопросы на экзамен №33-40 (МДК.02.01);
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	ЛР 1, ЛР 16, ЛР 22, ЛР 3, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6. (МДК.02.02);	Вопросы на экзамен №41-50 (МДК.02.02);
Применять математический аппарат для выполнения криптографических преобразований;	ЛР 1, ЛР 16, ЛР 22, ЛР 3, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6. (МДК.02.02);	Вопросы на экзамен №34-40 (МДК.02.02);
Проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;	ЛР 1, ЛР 16, ЛР 22, ЛР 3, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6. (МДК.02.02);	Вопросы на экзамен №25-33 (МДК.02.02);
Знание		
типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;	ЛР 13, ЛР 17, ЛР 18, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6. (МДК.02.01);	Вопросы на экзамен №17-24 (МДК.02.01);
методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;	ЛР 13, ЛР 17, ЛР 18, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6. (МДК.02.01);	Вопросы на экзамен №9=16 (МДК.02.01);
Особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;	ЛР 13, ЛР 17, ЛР 18, ЛР 23, ЛР 27, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6. (МДК.02.01);	Вопросы на экзамен №1-8 (МДК.02.01);
Типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.	ЛР 1, ЛР 16, ЛР 22, ЛР 3, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6. (МДК.02.02);	Вопросы на экзамен №16-24 (МДК.02.02);
особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;	ЛР 1, ЛР 16, ЛР 22, ЛР 3, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6. (МДК.02.02);	Вопросы на экзамен №8-15 (МДК.02.02);
основные понятия криптографии и типовых криптографических методов и средств защиты информации;	ЛР 1, ЛР 16, ЛР 22, ЛР 3, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6. (МДК.02.02);	Вопросы на экзамен №1-7 (МДК.02.02);