

**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**

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 2025 - 2026 учебный год.

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

Разработчики:

1. Кононова Наталия Владимировна

Рассмотрено и рекомендовано на заседании кафедры Информационной безопасности

Протокол №10 от 12.05.2025

Заведующий кафедрой Кононова Наталия Владимировна

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.**

1.1.1. Перечень общих компетенций

Код	Наименование общих компетенций
ОК 02.	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности
ОК 03.	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста
ОК 09.	Пользоваться профессиональной документацией на государственном и иностранном языках
ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 04.	Эффективно взаимодействовать и работать в коллективе и команде
ОК 06.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения
ОК 07.	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, 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

1.1.2. Перечень профессиональных компетенций

Код	Наименование профессиональных компетенций
ВД	- эксплуатация автоматизированных (информационных) систем в защищенном исполнении; - защита информации в автоматизированных системах программными и программно-аппаратными средствами; - защита информации техническими средствами.
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

1.2. 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:

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

Знание:

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

Иметь практический опыт:

- Отчет по учебной практике;
- правильно оформленный отчет;

1.3. Рекомендуемое количество часов на освоение программы профессионального модуля

Всего - 663 час(-а, -ов), в том числе:

самостоятельной работы обучающегося - 30 час(-а, -ов),

максимальной учебной нагрузки обучающегося - 633 час(-а, -ов), включая:

- обязательной аудиторной учебной нагрузки обучающегося - 633 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 обучающихся, курсовая работа (проект) (если предусмотрены)	Объём в часах	Уровень освоения	Коды компетенций, формированию которых способствует элемент программы
МДК.02.01 Программные и программно-аппаратные средства защиты информации		204		
Тема 1 Применение криптографических средств защиты информации в базах данных.	Содержание учебного материала 1 Лекционные занятия №1 16. Применение криптографических средств защиты информации в базах данных.	2	1	ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
Тема 2 Proxy-сервера прикладного уровня.	Содержание учебного материала 1 Лекционные занятия №2 8.Proxy-сервера прикладного уровня. 2 Практические занятия №1 7. Применение программ для шифрования данных на съемных носителях. 3 Практические занятия №2 7. Выбор мер защиты информации для их реализации в информационной системе. 4 Практические занятия №3 7. Изучение современных систем антивирусной защиты на примере корпоративных решений KasperskyLab или других аналогов.	2 2 2 2	1 2 2 2	ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
Тема 3 Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне.	Содержание учебного материала 1 Лекционные занятия №3 7. Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне. 2 Лекционные занятия №4 6. Применение программ для безвозвратного удаления данных 3 Практические занятия №4 6. Проведение аудита ЛВС сетевым сканером. 4 Практические занятия №5 6. Изучение типовых решений для построения VPN на примере VipNet или других аналогов	2 2 2 4	1 1 2 2	ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
Тема 4 Пакетные фильтры.	Содержание учебного материала 1 Лекционные занятия №5 6. Пакетные фильтры. 2 Лекционные занятия №6 5. Применение специализированного программно средства для восстановления удаленных файлов 3 Практические занятия №6 5. Изучение штатных средств защиты СУБД MSSQL Server 4 Практические занятия №7 5. Изучение функций и настройка режимов работы на примере MaxPatrol 8 или других аналогов	2 2 2 4	1 1 2 2	ПК 2.1., ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект) (если предусмотрены)	Объём в часах	Уровень освоения	Коды компетенций, формированию которых способствует элемент программы	
Тема 5 Основные типы firewall. Симметричные и несимметричные firewall.	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.	
	1	Лекционные занятия №7 4. Основные типы firewall. 5. Симметричные и несимметричные firewall.	2		1
	2	Практические занятия №8 4. Применение средства восстановления остаточной информации на примере Foremost или аналога	2		2
	3	Практические занятия №9 4. Изучение механизмов защиты СУБД MS Access	2		2
	4	Практические занятия №10 4. Установка и настройка программных средств оценки защищенности и аудита информационной безопасности.	4	2	
Тема 6 Достоинства, недостатки, реализуемые политики безопасности	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.	
	1	Лекционные занятия №8 3. Достоинства, недостатки, реализуемые политики безопасности	2		1
	2	Практические занятия №11 3. Защитные механизмы в приложениях (на примере MSWord, MSExcel, MSPowerPoint) Часть 2.	2		2
	3	Практические занятия №12 3. Изучение различных способов закрытия "опасных" портов.	2		2
	4	Практические занятия №13 3. Выбор соответствующих программных и программно-аппаратных средств и рекомендаций по их настройке.	2	2	
Тема 7 Межсетевые экраны типа firewall.	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.	
	1	Лекционные занятия №9 2. Межсетевые экраны типа firewall.	2		1
	2	Лабораторные занятия №1 2. Защитные механизмы в приложениях (на примере MSWord, MSExcel, MSPowerPoint) Часть 1.	2		2
	3	Практические занятия №14 2. Развертывание VPN.	2		2
	4	Практические занятия №15 2. Изучение и сравнительный анализ распространенных сетевых мониторов на примере RealSecure, SNORT, NFR или других аналогов	4	2	
Тема 8 Методы защиты информации при работе в сетях общего доступа.	Содержание учебного материала			ОК 01., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6., ОК 02., ОК 03.	
	1	Лекционные занятия №10 1. Методы защиты информации при работе в сетях общего доступа.	2		1
	2	Лабораторные занятия №2 1. Защита информации от несанкционированного копирования с использованием специализированных программных средств.	2		2
	3	Практические занятия №16 1. Моделирование проведения атаки. Изучение инструментальных средств обнаружения вторжений	2		2
	4	Практические занятия №17 1. Изучение и сравнение архитектур Dual Homed Host, Bastion Host, Perimetr.	4	2	
Тема 9 Понятие изолированной программной среды. Часть 2.	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.	
	1	Лекционные занятия №11 Понятие изолированной программной среды. Часть 2.	2		1
	2	Практические занятия №18 Исследование атаки переполнения буфера как примера нарушения конфиденциальности, целостности и доступности информации	2		2
	3	Практические занятия №19 Защита от вредоносного кода	2	2	

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект) (если предусмотрены)	Объём в часах	Уровень освоения	Коды компетенций, формированию которых способствует элемент программы	
Тема 10 Понятие изолированной программной среды. Часть 1.	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.	
	1	Лекционные занятия №12 Понятие изолированной программной среды. Часть 1.	2		1
	2	Практические занятия №20 Анализ информационной инфраструктуры государства.	2		2
	3	Практические занятия №21 Разработка программного обеспечения	2		2
	4	Практические занятия №22 Методы контроля конфигурации	2	2	
Тема 11 Компьютерные вирусы как особый класс разрушающих программных воздействий. Часть 2	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.	
	1	Лекционные занятия №13 Компьютерные вирусы как особый класс разрушающих программных воздействий. Часть 2	2		1
	2	Практические занятия №23 Источники угроз информационной безопасности Российской Федерации.	2		2
	3	Практические занятия №24 Нарушения функциональной целостности	2	2	
Тема 12 Компьютерные вирусы как особый класс разрушающих программных воздействий. Часть 1	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.	
	1	Лекционные занятия №14 Компьютерные вирусы как особый класс разрушающих программных воздействий. Часть 1	2		1
	2	Практическая подготовка №1 Виды угроз информационной безопасности Российской Федерации.	32	2	
Тема 13 Классификация и методы внедрения программных закладок	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.	
1	Лекционные занятия №15 Классификация и методы внедрения программных закладок	2	1		
Тема 14 Методы перехвата и навязывания информации	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.	
1	Лекционные занятия №16 Методы перехвата и навязывания информации	2	1		
Тема 15 Модели взаимодействия прикладной программы и программной закладки	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.	
1	Лекционные занятия №17 Модели взаимодействия прикладной программы и программной закладки	2	1		
Тема 16 Программа с потенциально опасными последствиями.	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.	
	1	Лекционные занятия №18 Программа с потенциально опасными последствиями.	2		1
	2	Практические занятия №25 Разные команды Windows	2	2	
Тема 17 Защита информации от разрушающих программных воздействий. Понятие разрушающего программного воздействия	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.	
1	Практические занятия №26 Защита информации от разрушающих программных воздействий. Понятие разрушающего программного воздействия	2	2		

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект) (если предусмотрены)	Объём в часах	Уровень освоения	Коды компетенций, формированию которых способствует элемент программы
Тема 18 Многоуровневая модель безопасности баз данных. Многозначность.	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 Практические занятия №27 Многоуровневая модель безопасности баз данных. Многозначность.	2	2	
Тема 19 Защита информации в базах данных. Часть 2.	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 Практические занятия №28 Защита информации в базах данных. Часть 2.	2	2	
Тема 20 Защита информации в базах данных. Часть 1	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 Практические занятия №29 Защита информации в базах данных. Часть 1	2	2	
Тема 21 Защита информации в операционной системе Linux	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 Лабораторные занятия №3 Защита информации в операционной системе Linux	2	2	
Тема 22 Защита информации в операционной системе Windows.	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 Лабораторные занятия №4 Защита информации в операционной системе Windows.	2	2	
Тема 23 Стандарты защищенности операционных систем.	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 Практические занятия №30 Стандарты защищенности операционных систем.	2	2	
	2 Часы на контроль Контроль	12	2	
Тема 24 Разграничение доступа к объектам операционной системы. Часть 2	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 Самостоятельная работа №1 Разграничение доступа к объектам операционной системы. Часть 2	2	3	
	2 Самостоятельная работа №2 Использование командных файлов Часть 2	2	3	
Тема 25 Разграничение доступа к объектам операционной системы. Часть 1	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 Самостоятельная работа №3 Разграничение доступа к объектам операционной системы. Часть 1	2	3	
	2 Самостоятельная работа №4 Использование командных файлов Часть 1	2	3	
Тема 26 Основные средства и методы защиты информации в операционной системе. Часть 1.	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 Самостоятельная работа №5 Основные средства и методы защиты информации в операционной системе. Часть 1.	2	3	
	2 Самостоятельная работа №6 Командные файлы и программирование	2	3	

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект) (если предусмотрены)	Объём в часах	Уровень освоения	Коды компетенций, формированию которых способствует элемент программы
Тема 27 Классификация угроз безопасности операционной системы	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 Самостоятельная работа №7 Классификация угроз безопасности операционной системы	2	3	
	2 Самостоятельная работа №8 Работа с файлами и каталогами	2	3	
Тема 28 Классификация методов и средств программно-аппаратной защиты информации	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 Самостоятельная работа №9 Классификация методов и средств программно-аппаратной защиты информации	2	3	
	2 Самостоятельная работа №10 Работа с каталогами	2	3	
Тема 29 Основные понятия программно-аппаратной защиты информации	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 Самостоятельная работа №11 Основные понятия программно-аппаратной защиты информации	2	3	
	2 Самостоятельная работа №12 Работа с файлами	2	3	
Тема 30 Средства аудита и контроля безопасности. Критерии защищенности баз данных	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 Лекционные занятия №19 15. Средства аудита и контроля безопасности. Критерии защищенности баз данных	2	1	
Тема 31 Средства контроля целостности информации в базах данных.	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 Лекционные занятия №20 14. Средства контроля целостности информации в базах данных.	2	1	
Тема 32 Средства идентификации и аутентификации. Управление доступом.	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 Лекционные занятия №21 13. Средства идентификации и аутентификации. Управление доступом.	2	1	
Тема 33 Основные типы угроз. Модель нарушителя.	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 Лекционные занятия №22 12. Основные типы угроз. Модель нарушителя.	2	1	
Тема 34 Требования по сертификации межсетевых экранов.	Содержание учебного материала			ПК 2.6., ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5.
	1 Лекционные занятия №23 11. Требования по сертификации межсетевых экранов.	2	1	
Тема 35 Требования к каждому хосту исходя из архитектуры и выполняемых функций	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 Лекционные занятия №24 10. Требования к каждому хосту исходя из архитектуры и выполняемых функций	2	1	

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект) (если предусмотрены)	Объём в часах	Уровень освоения	Коды компетенций, формированию которых способствует элемент программы
Тема 36 Основные типы архитектур мультимастерных firewall.	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 Лекционные занятия №25 9. Основные типы архитектур мультимастерных firewall.	2	1	
Тема 37 Одномастерные и мультимастерные firewall.	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 Лекционные занятия №26 8. Одномастерные и мультимастерные firewall.	2	1	
	2 Самостоятельная работа №13 8. Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов.	2	3	
3 Самостоятельная работа №14 8. Изучение функционала и областей применения DLP систем на примере InfoWatchTrafficMonitor или других аналогов.	4	3		
Курсовая работа		30	30	ОК 08., ОК 07., ОК 06., ОК 04., ОК 01., ОК 09., ОК 05., ОК 03., ОК 02., ПК 2.5., ПК 2.6., ПК 2.3., ПК 2.2., ПК 2.1., ПК 2.4.
Форма(-ы) контроля - 5 семестр, Экзамен; 4 семестр, Курсовая работа; 4 семестр, Курсовая работа				
Всего по МДК.02.01 Программные и программно-аппаратные средства защиты информации		204		
МДК.02.02 Криптографические средства защиты информации		146		
Тема 1 Промежуточная аттестация	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 Часы на контроль Промежуточная аттестация	18	2	

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект) (если предусмотрены)	Объём в часах	Уровень освоения	Коды компетенций, формированию которых способствует элемент программы
Тема 2 Практическая подготовка	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	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 рnr	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		

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект) (если предусмотрены)	Объём в часах	Уровень освоения	Коды компетенций, формированию которых способствует элемент программы
Тема 3 Практические занятия	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	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	4	2	
	6 Практические занятия №6 алгоритм блочного шифрования данных гост 28147-89	4	2	
	7 Практические занятия №7 симметричное и асимметричное шифрование данных средствами криптографического пакета openssl. Часть 1.	4	2	
	8 Практические занятия №8 симметричное и асимметричное шифрование данных средствами криптографического пакета openssl. Часть 2.	4	2	
	9 Практические занятия №9 шифрование сообщений с помощью шифров замены криптографическими функциями excel	4	2	
	10 Практические занятия №10 исследование работы простейших алгоритмов шифрования в среде программирования delphi	6	2	
	11 Практические занятия №11 исследование функций гаммирования на языке программирования java	4	2	

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект) (если предусмотрены)	Объём в часах	Уровень освоения	Коды компетенций, формированию которых способствует элемент программы
Тема 4 Лекции	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., 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 «считала»	2	1	
4	Лекционные занятия №4 Диск Энея. Квадрат Полибия	1	1	
5	Лекционные занятия №5 Шифр Чейза. Тюремный шифр	1	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	1	1	
15	Лекционные занятия №15 Практическая криптографическая стойкость	1	1	
16	Лекционные занятия №16 Классификация поточных шифров	1	1	
17	Лекционные занятия №17 Регистр сдвига с линейной обратной связью	1	1	
18	Лекционные занятия №18 Линейная сложность	1	1	
19	Лекционные занятия №19 Методы и способы криптографической защиты информации.	1	1	
20	Лекционные занятия №20 Инфраструктура открытых ключей (ИОК/РКИ).	1	1	
21	Лекционные занятия №21 Криптосистема	1	1	
22	Лекционные занятия №22 Сертификаты	1	1	
23	Лекционные занятия №23 Сети и сетевой доступ	1	1	
24	Лекционные занятия №24 Способы предотвращения удаленных атак на информационные системы	2	1	
25	Лекционные занятия №25 Защита от атак	2	1	
26	Лекционные занятия №26 Методы криптографии	2	1	
27	Лекционные занятия №27 Межсетевой экран	2	1	
28	Лекционные занятия №28 Фильтрация на сетевом уровне	2	1	
29	Лекционные занятия №29 Фильтрация на прикладном уровне	2	1	
30	Лекционные занятия №30 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 обучающихся, курсовая работа (проект) (если предусмотрены)	Объём в часах	Уровень освоения	Коды компетенций, формированию которых способствует элемент программы
Форма(-ы) контроля - 4 семестр, Экзамен				
Всего по МДК.02.02 Криптографические средства защиты информации		146		
УП.02.01 Учебная практика (Защита информации в автоматизированных системах программными и программно-аппаратными средствами)		108		
Тема 1 Ознакомительный этап	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 Практическая подготовка №1 Ознакомительный этап	6	2	
Тема 2 Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 Практическая подготовка №2 Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах	6	2	
Тема 3 Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 Практическая подготовка №3 Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности	6	2	
Тема 4 Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 Практическая подготовка №4 Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности	6	2	
Тема 5 Составление документации по учету, обработке, хранению и передаче конфиденциальной информации	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 Практическая подготовка №5 Составление документации по учету, обработке, хранению и передаче конфиденциальной информации	6	2	
Тема 6 Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 Практическая подготовка №6 Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации	6	2	

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект) (если предусмотрены)	Объём в часах	Уровень освоения	Коды компетенций, формированию которых способствует элемент программы
Тема 7 Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 Практическая подготовка №7 Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов	6	2	
Тема 8 Устранение замечаний по результатам проверки	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 Практическая подготовка №8 Устранение замечаний по результатам проверки	6	2	
Тема 9 Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов.	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 Практическая подготовка №9 Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов.	6	2	
Тема 10 Применение математических методов для оценки качества и выбора наилучшего программного средства	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 Практическая подготовка №10 Применение математических методов для оценки качества и выбора наилучшего программного средства	6	2	
Тема 11 Составление документации по учету, обработке, хранению и передаче конфиденциальной информации	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 Практическая подготовка №11 Составление документации по учету, обработке, хранению и передаче конфиденциальной информации	6	2	
Тема 12 Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 Практическая подготовка №12 Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации	6	2	
Тема 13 Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 Практическая подготовка №13 Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов	6	2	
Тема 14 Устранение замечаний по результатам проверки	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 Практическая подготовка №14 Устранение замечаний по результатам проверки	6	2	

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект) (если предусмотрены)	Объём в часах	Уровень освоения	Коды компетенций, формированию которых способствует элемент программы
Тема 15 Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов.	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 Практическая подготовка №15 Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов.	6	2	
Тема 16 Применение математических методов для оценки качества и выбора наилучшего программного средства	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 Практическая подготовка №16 Применение математических методов для оценки качества и выбора наилучшего программного средства	6	2	
Тема 17 Составление документации по учету, обработке, хранению и передаче конфиденциальной информации	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 Практическая подготовка №17 Составление документации по учету, обработке, хранению и передаче конфиденциальной информации	6	2	
Тема 18 Формирование отчетности о практике	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 Практическая подготовка №18 Формирование отчетности о практике	6	2	
Форма(-ы) контроля - 4 семестр, Дифференцированный зачет				
Всего по УП.02.01 Учебная практика (Защита информации в автоматизированных системах программными и программно-аппаратными средствами)		108		
ПП.02.01 Производственная практика (Защита информации в автоматизированных системах программными и программно-аппаратными средствами)		144		
Тема 1 Вводный инструктаж, знакомство с базой практики	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 Практическая подготовка №1 Требования по защите конфиденциальных данных предприятия	6	2	
Тема 2 Системы контроля и управления доступом на предприятии	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 Практическая подготовка №2 Способы предупреждения компьютерных атак	6	2	
	2 Практическая подготовка №3 Требования по защите персональных данных	6	2	
	3 Практическая подготовка №4 Способы ограничения доступа к информации	6	2	
	4 Практическая подготовка №5 Признаки наличия вредоносного программного обеспечения	6	2	
	5 Практическая подготовка №6 Средства обнаружения компьютерных атак	6	2	
	6 Практическая подготовка №7 Программно-аппаратные средства уничтожения информации и носителей информации	6	2	

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект) (если предусмотрены)	Объём в часах	Уровень освоения	Коды компетенций, формированию которых способствует элемент программы	
Тема 3 Профили защиты программных и программно-аппаратных средств	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.	
	1	Практическая подготовка №8 межсетевые экраны	4		2
	2	Практическая подготовка №9 средства контроля съемных машинных носителей информации	4		2
	3	Практическая подготовка №10 средства доверенной загрузки	4		2
	4	Практическая подготовка №11 средства антивирусной защиты	4		2
Тема 7 Особенности автоматизированных систем в защищенном исполнении.	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.	
	1	Практическая подготовка №12 Особенности автоматизированных систем в защищенном исполнении.	6		2
	2	Практическая подготовка №13 Основные виды АС в защищенном исполнении.	6		2
	3	Практическая подготовка №14 Методы создания безопасных систем.	6		2
	4	Практическая подготовка №15 Методология проектирования гарантированно защищенных КС.	6		2
	5	Практическая подготовка №16 Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам.	6		2
	6	Практическая подготовка №17 Доступ к данным со стороны процесса.	6		2
	7	Практическая подготовка №18 Особенности защиты данных от изменения. Шифрование.	6		2
	8	Практическая подготовка №19 Работа с автономной АС в защищенном режиме.	6		2
Тема 8 Защита ОС	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.	
	1	Практическая подготовка №20 Алгоритм загрузки ОС. Штатные средства замыкания среды.	6		2
	2	Практическая подготовка №21 Расширение BIOS как средство замыкания программной среды.	6		2
	3	Практическая подготовка №22 Системы типа Электронный замок. ЭЗ с проверкой целостности программной среды. АМДЗ (доверенная загрузка).	6		2

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект) (если предусмотрены)	Объём в часах	Уровень освоения	Коды компетенций, формированию которых способствует элемент программы
Тема 9 Защита ПО	Содержание учебного материала			ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ПК 2.1., ПК 2.2., ПК 2.3., ПК 2.4., ПК 2.5., ПК 2.6.
	1 Практическая подготовка №23 Изучение и обратное проектирование ПО. Способы изучения ПО: статическое и динамическое изучение.	6	2	
	2 Практическая подготовка №24 Задачи защиты от изучения и способы их решения. Защита от отладки. Защита от дизассемблирования. Защита от трассировки по прерываниям. Вредоносное программное обеспечение как особый вид разрушающих воздействий.	6	2	
	3 Практическая подготовка №25 Классификация вредоносного программного обеспечения. Схема заражения. Средства нейтрализации вредоносного ПО. Профилактика заражения. Поиск следов активности вредоносного ПО.	6	2	
	4 Практическая подготовка №26 Реестр Windows. Основные ветки, содержащие информацию о вредоносном ПО. Другие объекты, содержащие информацию о вредоносном ПО, файлы prefetch.	2	2	
Форма(-ы) контроля - 6 семестр, Дифференцированный зачет				
Всего по ПП.02.01 Производственная практика (Защита информации в автоматизированных системах программными и программно-аппаратными средствами)		144		
Всего по ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами		663		

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:

Лекционная аудитория

- Проектор (1 шт.)

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

Лаборатория информационных технологий, сетей и систем передачи информации, программирования и баз данных

- Компьютерный стол (15 шт.)
- Стул (15 шт.)
- Доска (1 шт.)
- Системный блок (15 шт.)
- Монитор (15 шт.)
- Клавиатура (15 шт.)
- Компьютерная мышь (15 шт.)

Реализация УП.02.01 Учебная практика (Защита информации в автоматизированных системах программными и программно-аппаратными средствами) предполагает наличие помещений:

Компьютерный класс

Кабинет информатики (компьютерные классы)

Лаборатория информационно-коммуникационных систем

Лаборатория управления проектной деятельностью

- Системный блок (15 шт.)
- Монитор (15 шт.)
- Клавиатура (15 шт.)
- Компьютерная мышь (15 шт.)
- стол преподавателя (1 шт.)

- Компьютерный стол (15 шт.)
- стул (15 шт.)
- доска (1 шт.)

Реализация ПП.02.01 Производственная практика (Защита информации в автоматизированных системах программными и программно-аппаратными средствами) предполагает наличие помещений:

База практики

- Комплект оборудования для практики в соответствии с профессиональным модулем (1 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. Егошина, И. Л. Средства и методы обеспечения безопасности объектов и защиты информации : практикум / И. Л. Егошина. - Йошкар-Ола : Поволжский государственный технологический университет, 2021. - 158 с. - ISBN 978-5-8158-2240-5. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1894515>

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. Маршаков, Д. В. Методы и средства криптографической защиты информации. Практический курс : учебное пособие / Д.В. Маршаков, Д.В. Фахти. — Москва : ИНФРА-М, 2022. — 76 с. — (Высшее образование). - ISBN 978-5-16-110842-0. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/1891129>

Дополнительная литература:

1. Егошина, И. Л. Средства и методы обеспечения безопасности объектов и защиты информации : практикум / И. Л. Егошина. - Йошкар-Ола : Поволжский государственный технологический университет, 2021. - 158 с. - ISBN 978-5-8158-2240-5. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1894515>

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 **УП.02.01 Учебная практика (Защита информации в автоматизированных системах программными и программно-аппаратными средствами):**

Основная литература:

- 1.

Дополнительная литература:

- 1.

Информационные справочно-правовые системы и ресурсы:

1.

Перечень рекомендуемых учебных изданий и дополнительной литературы для **ПП.02.01 Производственная практика (Защита информации в автоматизированных системах программными и программно-аппаратными средствами)**:

Основная литература:

1. 1. Ильин М. Е., Калинкина Т. И., Пржегорлинский В.Н. Криптографическая защита информации в объектах информационной инфраструктуры, 1-е изд., ИЦ АКАДЕМИЯ, 2020 - 288 с.
2. 2. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 2-е изд., испр. и доп. — М.: Издательство Юрайт, 2020. — 240 с.

Дополнительная литература:

1. 1. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 2020 г. № 608.
2. 2. 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 2023 г. № 21.
3. 3. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2024 г.
4. 4. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2022 г. № 83.
5. 5. 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 2022 г. № 84.
6. 6. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2022 г. № 282.
7. 7. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2023 г. № 17.
8. 8. Требования о защите информации, содержащейся в информационных

системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России

9. от 31 августа 2020 г. № 416/489.

10. 9. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2021 г. № 638.

Информационные справочно-правовые системы и ресурсы:

1.

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	
ОК 02. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях	- демонстрация ответственности за принятые решения - обоснованность самоанализа и коррекция результатов собственной работы;	
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста	- грамотность устной и письменной речи, - ясность формулирования и изложения мыслей	
ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	- обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач	
ОК 04. Эффективно взаимодействовать и работать в коллективе и команде	- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных)	
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения	- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик,	
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, 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 поддержания необходимого уровня физической подготовленности	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик;	

Результаты (освоенные профессиональные и общие компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
ПК		тестирование, экзамен квалификационный, экспертное наблюдение в выполнении лабораторных работ, экспертное наблюдение в выполнении 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	
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	
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	
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	
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	Проявлять знания и умения в защите автоматизированных (информационных) систем 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	Демонстрация алгоритма проведения работ по уничтожению информации и носителей информации с использованием программных и программно-аппаратных средств	

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		
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, настраивать, применять программные и программно-аппаратные средства защиты информации;	Уметь устанавливать, настраивать, применять программные и программно-аппаратные средства 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
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
Применять математический аппарат для выполнения криптографических преобразований;	Уметь применять математический аппарат для выполнения криптографических преобразований;	Тестирование
Знание		

Наименование образовательного результата	Показатели оценки результата	Формы и методы контроля и оценки результата
методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;	Знать методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;	Коллоквиум
типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;	Знать типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;	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
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
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
Иметь практический опыт		
Отчет по учебной практике	Защита отчета по учебной практике	проверка отчета
правильно оформленный отчет	5 - описаны оба задания 4 - недостатки в оформлении отчета 3 - отсутствует одно из заданий	проверка отчета

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

Результаты обучения	Коды компетенций	Фонды оценочных средств
Умение		
диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;	ПК 2.6., ПК 2.5., ПК 2.4., ПК 2.3., ПК 2.2., ПК 2.1., ОК 09., ОК 08., ОК 07., ОК 06., ОК 05., ОК 04., ОК 03., ОК 02., ОК 01. (МДК.02.01);	Вопросы на экзамен №41-50 (МДК.02.01);
устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;	ПК 2.6., ПК 2.5., ПК 2.4., ПК 2.3., ПК 2.2., ПК 2.1., ОК 09., ОК 08., ОК 07., ОК 06., ОК 05., ОК 04., ОК 03., ОК 02., ОК 01. (МДК.02.01);	Вопросы на экзамен №25-32 (МДК.02.01);
устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;	ПК 2.6., ПК 2.5., ПК 2.4., ПК 2.3., ПК 2.2., ПК 2.1., ОК 09., ОК 08., ОК 07., ОК 06., ОК 05., ОК 04., ОК 03., ОК 02., ОК 01. (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	ПК 2.6., ПК 2.5., ПК 2.4., ПК 2.3., ПК 2.2., ПК 2.1., ОК 09., ОК 08., ОК 07., ОК 06., ОК 05., ОК 04., ОК 03., ОК 02., ОК 01. (МДК.02.02);	Вопросы на экзамен №41-50 (МДК.02.02);
Проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;	ПК 2.6., ПК 2.5., ПК 2.4., ПК 2.3., ПК 2.2., ПК 2.1., ОК 09., ОК 08., ОК 07., ОК 06., ОК 05., ОК 04., ОК 03., ОК 02., ОК 01. (МДК.02.02);	Вопросы на экзамен №25-33 (МДК.02.02);

Результаты обучения	Коды компетенций	Фонды оценочных средств
Применять математический аппарат для выполнения криптографических преобразований;	ПК 2.6., ПК 2.5., ПК 2.4., ПК 2.3., ПК 2.2., ПК 2.1., ОК 09., ОК 08., ОК 07., ОК 06., ОК 05., ОК 04., ОК 03., ОК 02., ОК 01. (МДК.02.02);	Вопросы на экзамен №34-40 (МДК.02.02);
Знание		
методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;	ПК 2.6., ПК 2.5., ПК 2.4., ПК 2.3., ПК 2.2., ПК 2.1., ОК 09., ОК 08., ОК 07., ОК 06., ОК 05., ОК 04., ОК 03., ОК 02., ОК 01. (МДК.02.01);	Вопросы на экзамен №9-16 (МДК.02.01);
типичные модели управления доступом, средств, методов и протоколов идентификации и аутентификации;	ПК 2.6., ПК 2.5., ПК 2.4., ПК 2.3., ПК 2.2., ПК 2.1., ОК 09., ОК 08., ОК 07., ОК 06., ОК 05., ОК 04., ОК 03., ОК 02., ОК 01. (МДК.02.01);	Вопросы на экзамен №17-24 (МДК.02.01);
Особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;	ПК 2.6., ПК 2.5., ПК 2.4., ПК 2.3., ПК 2.2., ПК 2.1., ОК 09., ОК 08., ОК 07., ОК 06., ОК 05., ОК 04., ОК 03., ОК 02., ОК 01. (МДК.02.01);	Вопросы на экзамен №1-8 (МДК.02.01);
особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;	ПК 2.6., ПК 2.5., ПК 2.4., ПК 2.3., ПК 2.2., ПК 2.1., ОК 09., ОК 08., ОК 07., ОК 06., ОК 05., ОК 04., ОК 03., ОК 02., ОК 01. (МДК.02.02);	Вопросы на экзамен №8-15 (МДК.02.02);
основные понятия криптографии и типовых криптографических методов и средств защиты информации;	ПК 2.6., ПК 2.5., ПК 2.4., ПК 2.3., ПК 2.2., ПК 2.1., ОК 09., ОК 08., ОК 07., ОК 06., ОК 05., ОК 04., ОК 03., ОК 02., ОК 01. (МДК.02.02);	Вопросы на экзамен №1-7 (МДК.02.02);
Типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.	ПК 2.6., ПК 2.5., ПК 2.4., ПК 2.3., ПК 2.2., ПК 2.1., ОК 09., ОК 08., ОК 07., ОК 06., ОК 05., ОК 04., ОК 03., ОК 02., ОК 01. (МДК.02.02);	Вопросы на экзамен №16-24 (МДК.02.02);
Иметь практический опыт		
Отчет по учебной практике	(УП.02.01);	(УП.02.01);
правильно оформленный отчет	ПК 2.6., ПК 2.5., ПК 2.4., ПК 2.3., ПК 2.2., ПК 2.1., ОК 09., ОК 08., ОК 07., ОК 06., ОК 05., ОК 04., ОК 03., ОК 02., ОК 01. (ПП.02.01);	(ПП.02.01);