МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«Национальный исследовательский ядерный университет «МИФИ»

Димитровградский инженерно-технологический институт –

филиал федерального государственного автономного образовательного учреждения высшего образования
«Национальный исследовательский ядерный университет «МИФИ»

(ДИТИ НИЯУ МИФИ)

СОГЛАСОВАНО
От работодателя:
Зам. директора ООО "АИС Город"
должность, название предприятия
_____ Р.Н. Насальник
«15» апреля 2022 г.
М.П.

УТВЕРЖДАЮ
Руководитель ДИТИ НИЯУ МИФИ
должность и название образовательного учреждения
_____ И.И. Бегинина
«12» мая 2022 г.
М.П.

Рабочая программа

учебной дисциплины МДК.02.01 Программные и программно-аппаратные средства защиты информации

по программе подготовки специалистов среднего звена

специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Форма обучения очная Учебный цикл ПМ

Составитель рабочей программы: А.С. Аверьянов, преподаватель техникума ДИТИ НИЯУ МИФИ

Димитровград

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.02 АРХИТЕКТУРА КОМПЬЮТЕРНЫХ СИСТЕМ

1.1. Область применения программы

Примерная программа учебной дисциплины является частью примерной основной образовательной программы в соответствии с ФГОС СПО ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем", утвержденном приказом Минобрнауки РФ от 9 декабря 2016 г. № 1553

1.2. Место дисциплины в структуре ППССЗ

Учебная дисциплина относится к обязательной части ППССЗ и принадлежит к циклу дисциплин профессионального модуля и является базой для освоения практик.

1.3. Цель и планируемые результаты освоения дисциплины:

В результате освоения дисциплины обучающийся должен

иметь практический опыт:

- участия в эксплуатации систем и средств защиты информации защищаемых объектов;
- применения технических средств защиты информации;
- выявления возможных угроз информационной безопасности объектов защиты;

знать:

- общие типы проблем, которые могут возникнуть при разработке программного обеспечения;
- общие типы проблем, которые могут возникнуть в коммерческой организации; *
- диагностические подходы к решению проблем;
- тенденции и разработки в отрасли, включая новые платформы, языки, условные обозначения и технические навыки.
- важность рассмотрения всех возможных вариантов и выбора лучшего решения на основе взвешенного аналитического суждения и интересов клиента;
- важность использования системного анализа и методологий проектирования (например, унифицированного языка моделирования (Unified Modelling Language), программной платформы MVC (Model-View-Control), фреймворки, шаблоны проектирования);
- необходимость быть в курсе новых технологий и принимать решение о целесообразности их применения;

уметь:

Использовать аналитические навыки для:

- синтезировать сложную или неоднородную информацию;
- определять функциональные и нефункциональные требования спецификации.

Использовать навыки исследования и обучения для:

- получать пользовательские требования (например, опросы, анкеты, поиск и анализ документов, совместная разработка приложения и наблюдение);
- независимо исследовать возникшие проблемы.

Самостоятельно решать проблемы, с которыми

- столкнулся в процессе работы:
- своевременно идентифицировать и решать проблемы;
- грамотно собирать и анализировать информацию;
- разрабатывать альтернативы для принятия решений, выбирать наиболее уместные варианты и реализовать необходимое решение.

владеть:

- профессиональной терминологией:
- навыками внедрения и эксплуатации современных средств программно-аппаратной защиты информации;

- способами выявления и нейтрализации программ разрушающего действия;
- навыками разработки и использования межсетевых экранов и систем обнаружения и предотвращения вторжений.

В результате освоения дисциплины обучающийся осваивает элементы компетенций:

ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
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 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в профессиональной деятельности и поддержания необходимого уровня физической подготовленности
ОК 09	Использовать информационные технологии в профессиональной деятельности
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языке
ПК 2.1	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации
ПК 2.2	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами
ПК 2.3	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации
ПК 2.4	Осуществлять обработку, хранение и передачу информации ограниченного доступа
ПК 2.5	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств
ПК 2.6	Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объем часов**
Общая учебная нагрузка	159
Самостоятельная работа	-
Обязательная учебная нагрузка	157
в том числе:	
теоретическое обучение	76
лабораторные занятия (если предусмотрено)	Не предусмотрена
практические занятия (если предусмотрено)	81
курсовая работа (проект) (если предусмотрено)	Не предусмотрена
контрольная работа	Не предусмотрена
Консультации	Не предусмотрена
Промежуточная аттестация (дифференцированный зачёт)	2

2.2. Тематический план и содержание учебной дисциплины «Программные и программно-аппаратные средства защиты информации»

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся		Объем часов	Осваиваемые элементы компетенций
1	2		3	4
Раздел 1. Технология применения технических методов и средств защиты информации			100	
Тема 1.1. Основные свойства информации как предмета защиты	Содержание учебного материала	Уровень освоения	4	
	Виды информации, защищаемой техническими средствами. Свойства информации, влияющие на возможности ее защиты	4	4	
	Тематика практических занятий и лабораторных работ		2	
	Практическое занятие № 1. Классификация устройств защиты информации. Изучение типовых методов работы.		2	
	Контрольные работы не предусмотрены			
Тема 1.2 Демаскирующие признаки объектов защиты	Содержание учебного материала	Уровень освоения	8	
	Классификация демаскирующих признаков. Опознавательные признаки и признаки деятельности объектов.	2	2	
	Видовые, сигнальные и вещественные демаскирующие признаки. Информативность признаков	4	4	
	Система защиты информации от несанкционированного доступа Страж NT 3.0. СЗИ СтронгДиск Про	2	2	
	Тематика практических занятий и лабораторных работ		2	
	Практическое занятие № 2. Изучение генераторов низкой/высокой частоты, импульсного генератора		2	
	Контрольные работы не предусмотрены			
Тема 1.3 Источники и носители конфиденциальной информации	Содержание учебного материала	Уровень освоения	6	
	Понятие архитектуры вычислительных систем.	2	2	
	Понятие об источниках, носителях и получателях информации. Классификация источников информации. Виды носителей	4	4	

	информации (люди, физические поля, электрические сигналы и материальные тела)			
	Тематика практических занятий и лабораторных работ		2	
	Практическое занятие № 3 Организация охраны и защиты выделенного помещения		2	
	Контрольные работы не предусмотрены			
Тема 1.4 Источники опасных сигналов	Содержание учебного материала	Уровень освоения	8	
	Понятие об опасном сигнале и их источниках. Основные и вспомогательные технические средства, и системы	4	4	
	Побочные электромагнитные излучения и наводки. Акустоэлектрические преобразователи, их виды и принципы работы	4	4	
	Тематика практических занятий и лабораторных работ		2	
	Практическое занятие № 4. Изучение виртуального цифрового осциллографа. Тестеры		2	
	Контрольные работы не предусмотрены			
Тема 1.5 Способы несанкционированного доступа к источникам информации	Содержание учебного материала	Уровень освоения	4	
	Понятие о разведывательном контакте и его условиях. Принципы доступа к источникам информации без физического проникновения в контролируемую зону	4	4	
	Тематика практических занятий и лабораторных работ		2	
	Практическое занятие № 5. Защищенные соединения. Удаленное управление инженерно-техническими средствами		2	
	Контрольные работы не предусмотрены			
Тема 1.6 Способы и средства перехвата сигналов	Содержание учебного материала	Уровень освоения	6	
	Задачи, решаемые при перехвате сигналов. Структура средств перехвата и их функции.	4	4	
	Принципы определения координат источников радиоизлучений и анализа сигналов	2	2	
	Тематика практических занятий и лабораторных работ		2	

	Практическое занятие № 6. Изучение и обнаружение закладных аудиоустройств. Подавители диктофонов, генераторы белого и речеобразного шума.		2	
	Контрольные работы не предусмотрены			
Тема 1.7 Способы и средства подслушивания акустических сигналов	Содержание учебного материала	Уровень освоения	6	
	Структура и характеристики технических средств подслушивания.	2	2	
	Варианты камуфлирования закладных устройств. Способы и средства лазерного подслушивания и ВЧ-навязывания	4	4	
	Тематика практических занятий и лабораторных работ		2	
	Практическое занятие № 7. Изучение и обнаружение закладных аудиоустройств. Дифференциальный адаптер проводных линий ДАПЛ		2	
	Контрольные работы не предусмотрены			
Тема 1.8 Технические каналы утечки информации	Содержание учебного материала	Уровень освоения	6	
	Характеристики каналов утечки информации. Типовая структура технического канала утечки информации. Оптические каналы утечки информации	4	4	
	Радиоэлектронные каналы утечки информации	2	2	
	Тематика практических занятий и лабораторных работ		2	
	Практическое занятие № 8. Изучение радиолокаторов		2	
	Контрольные работы не предусмотрены			
Тема 1.9 Концепция технической защиты информации	Содержание учебного материала	Уровень освоения	8	
	Применение комплекса радиоконтроля спектр МК	4	4	
	Применение нелинейного радиолокатора NR-м	4	4	
	Тематика практических занятий и лабораторных работ			
	Контрольные работы не предусмотрены			
Тема 1.10 Способы и средства инженерной защиты и технической охраны	Содержание учебного материала	Уровень освоения	8	
	Модели злоумышленников. Уровни физической безопасности объектов охраны. Показатели эффективности инженерно-технической охраны объектов	2	2	
	Способы и средства инженерной защиты объектов.	2	2	

	Съем и защита информации по телефонной сети. Блокираторы и подавители сигнала сети сотовых телефонов. ГШ-1000У (генератор шума для защиты объектов вычислительной техники 1, 2 и 3 категорий от утечки информации)	4	4	
	Тематика практических занятий и лабораторных работ		2	
	Практическое занятие № 9. Съем и защита информации в вычислительной сети. Устройства защиты от утечки по каналам ПЭМИН. Устройства «зашумления» локальных компьютерных сетей.		2	
	Контрольные работы не предусмотрены			
Тема 1.11 Способы и средства защиты информации на предприятии	Содержание учебного материала	Уровень освоения	8	
	Способы и средства противодействия наблюдению в оптическом диапазоне волн. Особенности маскировки в видимом и ИК-диапазонах света	2	2	
	Способы и средства противодействия радиолокационному и гидроакустическому наблюдению. Способы активного подавления сигналов радиолокаторов	2	2	
	Съем и защита информации в вычислительной сети. Блокираторы Bluetooth и WiFi. Многофункциональный поисковый прибор ПИРАНЬЯ-Р	4	4	
	Тематика практических занятий и лабораторных работ		2	
	Практическое занятие № 10. Съем и защита информации по радиоканалу. Подавители радиомикрофонов и видеопередатчиков. Комплексные устройства защиты переговоров		2	
	Контрольные работы не предусмотрены			
Тема 1.12 Организационные и технические меры по технической защите информации в организации	Содержание учебного материала	Уровень освоения	6	
	Краткая характеристика государственной системы защиты информации. Основные руководящие и нормативные документы по организации технической защиты информации в организации, их сущность	2	2	
	Виды моделей угроз информации: путей физического проникновения злоумышленника к источнику и каналам утечки. Методические рекомендации по моделированию каналов утечки.	2	2	

	Формы представления результатов моделирования. Рекомендации по оценке угроз безопасности информации			
	Съем и защита информации по телефонной сети. Устройства защиты от прослушивания проводных телефонных линий. Устройства защиты от прослушивания сотовых телефонов	2	2	
	Тематика практических занятий и лабораторных работ		2	
	Практическое занятие № 11. Съем и защита информации по электросети. Сетевые помехоподавляющие фильтры и генераторы		2	
	Контрольные работы не предусмотрены			
Раздел 2. Технология использования программно-аппаратных средств защиты информации			58	
Тема 2.1. Назначение и задачи программно-аппаратной защиты информации	Содержание учебного материала	Уровень освоения	6	
	Цели и задачи программно-аппаратной защиты информации.	2	2	
	Службы защиты информации	2	2	
	Криптографическая защита информации	2	2	
	Тематика практических занятий и лабораторных работ		2	
	Практическое занятие № 12. Меры противодействия несанкционированному доступу		2	
	Контрольные работы не предусмотрены			
Тема 2.2. Принципы программно-аппаратной защиты информации от несанкционированного доступа	Содержание учебного материала	Уровень освоения	6	
	Основные подходы к ПА защите данных от несанкционированного доступа (НСД)	2	2	
	Защита сетевого файлового ресурса, фиксация доступа к файлам, доступ к данным со стороны процесса.	2	2	
	Создание защищенных логических дисков	2	2	
	Тематика практических занятий и лабораторных работ		2	
	Практическое занятие № 13 Работа с защищенными дисками		2	
	Контрольные работы не предусмотрены			
Тема 2.3. Программно-аппаратные средства шифрования	Содержание учебного материала	Уровень освоения	6	
	Построение аппаратных компонентов криптозащиты данных. Защита файлов от изменения.	2	2	

	Электронная цифровая подпись.	2	2	
	Система защиты информации от несанкционированного доступа «Страж NT»	2	2	
	Тематика практических занятий и лабораторных работ		2	
	Практическое занятие № 14 Запуск и регистрация в системе защиты		2	
	Контрольные работы не предусмотрены			
Тема 2.4. Программно-аппаратные методы и средства ограничения доступа к компонентам инфокоммуникационных систем	Содержание учебного материала	Уровень освоения	8	
	Дискреционный метод организации разграничения доступа.	2	2	
	Средства защиты программного обеспечения от несанкционированной загрузки.	2	2	
	Реализация мандатной модели разграничения доступа	4	4	
	Тематика практических занятий и лабораторных работ			
	Контрольные работы не предусмотрены			
Тема 2.5. Безопасность современных сетевых технологий	Содержание учебного материала	Уровень освоения	8	
	Классификация способов несанкционированного доступа и жизненный цикл атак.	2	2	
	Основные схемы сетевой защиты на базе межсетевых экранов.	2	2	
	Режим замкнутой программной среды	4	4	
	Тематика практических занятий и лабораторных работ			
	Контрольные работы не предусмотрены			
Тема 2.6. Безопасность в открытых сетях	Содержание учебного материала	Уровень освоения	8	
	Web-приложения. Стандарты в области ИОК.	2	2	
	Инфраструктура на основе криптографии с открытыми ключами (ИОК).	4	4	
	Настройка механизма шифрования	2	2	
	Тематика практических занятий и лабораторных работ			
	Контрольные работы не предусмотрены			
Тема 2.7. Программно-аппаратная защита от разрушающих программных воздействий	Содержание учебного материала	Уровень освоения	8	
	Компьютерные вирусы как особый класс разрушающих	4	4	

	программных воздействий.			
	Понятие изолированной программной среды.	4	4	
	Тематика практических занятий и лабораторных работ		2	
	Практическое занятие № 15. Гарантированное удаление данных		2	
	Контрольные работы не предусмотрены			
ВСЕГО			157	
Дифференцированный зачёт			2	

Для характеристики уровня освоения учебного материала используются следующие обозначения:

1. – ознакомительный (узнавание ранее изученных объектов, свойств);
2. – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством)
3. – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач)

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы дисциплины требует наличия Полигона вычислительной техники (ауд. 47)

Оборудование полигона:

- рабочее место преподавателя, оборудованное персональным компьютером с лицензионным или свободным программным обеспечением, соответствующим разделам программы, подключенным к сети Internet и средствами вывода звуковой информации;
- посадочные места по количеству обучающихся;
- комплект учебно-наглядных пособий «Архитектура компьютерных систем».

Технические средства обучения:

- компьютеры INTEL CELERON с лицензионным программным обеспечением;
- мультимедиапроектор Acer XI230;
- экран PAPER LUMA 127*16;
- периферийные устройства:
  - принтер SAMSUNG ML 1210;
  - сканер EPSON 1210

3.2. Информационное обеспечение обучения

1. Креопалов В.В., Технические средства и методы защиты информации: учебно-практическое пособие – М.: Изд.центр ЕАОИ, 2011.
2. Д.А. Скрипник, Общие вопросы технической защиты информации – М.: Национальный Открытый Университет «ИНТУИТ», 2016.
3. Пролетарский А.В., Смирнова Е.В., Суворов А.М., Технологии защиты информации в компьютерных сетях – М.: Национальный Открытый Университет «ИНТУИТ», 2016.
4. Башлы П.Н., Бабаш А.В., Баранова Е.К., Информационная безопасность и защита информации– М.: РИОР, 2013.
5. Савельев И.А. Программно-аппаратная защита информации: Учебное пособие / И.А. Савельев; Финуниверситет, Каф. информационной безопасности - М.: Финуниверситет, 2014.
6. Федеральный закон «Об информации, информационных технологиях и о защите информации». Собрание законодательства Российской Федерации 08.07.2006г.
7. Мельников В.П. Информационная безопасность. М.: Издательский центр «Академия», 2011.
8. Румынина Л.А. Документационное обеспечение управления. М.,ОИЦ «Академия». 2011.
9. Постановление Правительства РФ от 16 апреля 2012 года № 313 “Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)”.
10. Савельев И.А. Программно-аппаратная защита информации: Учебное пособие; Финуниверситет, Каф. информационной безопасности - М.: Финуниверситет, 2014.
11. Грибунин В.Г., Чудовский В.В.Комплексная система защиты информации на предприятии – Спб.: «Академия», 2013.

12. Бабаш А.В., Баранова Е.К., Мельников Ю.Н. Информационная безопасность. Практикум. Учебное пособие, Изд.: КноРус, 2016.

Дополнительные источники:

1. Хорев П.Б. Программно-аппаратная защита информации: учебное пособие / ЭБС ZNANIUM - Москва: Издательство "ФОРУМ", 2009.
2. Царегородцев А.В. Системы контроля доступа: Учебное пособие/ВГНА Минфина России - М.: ВГНА Минфина России, 2008.
3. Галатенко В. А. Стандарты информационной безопасности. — М.: Интернет-университет информационных технологий, 2009.
4. Биометрические системы безопасности/Ю.И.Лебеденко. – Тула: Издательство ТулГУ, 2012.
5. Партыка Т.Л., Попов И.И. Информационная безопасность. Учебное пособие, имеется гриф МО РФ, 2011.
6. Шаханова М.В. Современные технологии информационной безопасности: учебно-методический комплекс. – Москва: Проспект, 2015.
7. Галатенко В.А., Основы информационной безопасности – М.: Национальный Открытый Университет «ИНТУИТ», 2016.
8. Грибунин В.Г., Чудовский В.В., Комплексная система защиты информации на предприятии – Спб.: «Академия», 2010.

Периодические издания:

1 «CHIP»;
2 «JET INFO»;
3 «Грани безопасности»;
4 «Защита информации. Конфидент».

Интернет ресурсы:

1. Википедия – свободная энциклопедия – ru.wikipedia.org;
2. Издание о высоких технологиях – cnews.ru;
3. Российский сайт корпорации Microsoft – www.microsoft.com/rus
4. Каталог образовательных Интернет-ресурсов: учебно-методические пособия – edu/ru/modules.php
5. Электронный учебник по информатике и информационным технологиям – ctc.msiu.ru
6. Центр информационной безопасности - bezpeka.com
7. Дидактические и методические разработки по основам информатизации – studfiles.ru
8. Справочные материалы по техническим средствам информатизации – intuit.ru
9. Российская научная библиотека – rsl.ru

4 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе проведения практических занятий и лабораторных работ, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов.

Результаты обучения (освоенные умения, усвоенные знания)	Формы и методы контроля и оценки результатов обучения	Наименование тем
уметь: Использовать аналитические навыки для: - синтезировать сложную или неоднородную информацию; - определять функциональные и нефункциональные требования спецификации. Использовать навыки исследования и обучения для: - получать пользовательские требования (например, опросы, анкеты, поиск и анализ документов, совместная разработка приложения и наблюдение); - независимо исследовать возникшие проблемы. Самостоятельно решать проблемы, с которыми - столкнулся в процессе работы: - своевременно идентифицировать и решать проблемы; - грамотно собирать и анализировать информацию; - разрабатывать альтернативы для принятия решений, выбирать наиболее уместные варианты и реализовать необходимое решение. - участвовать в эксплуатации систем и средств защиты информации защищаемых объектов; - применять технические средства защиты информации; - выявлять возможные угрозы информационной безопасности объектов защиты;	Теоретический зачёт Компьютерное тестирование Практическое занятие Теоретический зачёт Компьютерное тестирование Практическое занятие Теоретический зачёт Компьютерное тестирование	Раздел 1. Представление информации в вычислительных системах. Раздел 2. Архитектура и принципы работы основных логических блоков вычислительных систем. Раздел 3. Вычислительные системы.
знать: - общие типы проблем, которые могут возникнуть при разработке программного обеспечения; - общие типы проблем, которые могут возникнуть в коммерческой организации; * - диагностические подходы к решению проблем;	Теоретический зачёт Компьютерное тестирование Практическое занятие	Раздел 1. Представление информации в вычислительных системах.

- тенденции и разработки в отрасли, включая новые платформы, языки, условные обозначения и технические навыки. - важность рассмотрения всех возможных вариантов и выбора лучшего решения на основе взвешенного аналитического суждения и интересов клиента; - важность использования системного анализа и методологий проектирования (например, унифицированного языка моделирования (Unified Modelling Language), программной платформы MVC (Model-View-Control), фреймворки, шаблоны проектирования); - необходимость быть в курсе новых технологий и принимать решение о целесообразности их применения;	Теоретический зачёт Компьютерное тестирование Практическое занятие Теоретический зачёт Компьютерное тестирование	Раздел 2. Архитектура и принципы работы основных логических блоков вычислительных систем. Раздел 3. Вычислительные системы.

5 ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ПРОГРАММЫ В ДРУГИХ ПООП

Рабочая программа по учебной дисциплине МДК.02.01 Программные и программно-аппаратные средства защиты информации может быть использована в любой ОПОП для УГС 09.00.00 и УГС 10.00.00 в качестве дисциплины профессионального модуля.