МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Колледж

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ МДК.02.01. ПРОГРАММНЫЕ И ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

по программе подготовки специалистов среднего звена (ППССЗ) среднего профессионального образования

Специальность:	*10.02.05.Обеспечение информационной безопасности автоматизированных систем*
Обучение:	*по программе базовой подготовки*
Уровень образования, на базе которого осваивается ППССЗ:	*среднее общее образование*
Квалификация:	*техник по защите информации*
Форма обучения:	*очная*

Махачкала - 2021

Рабочая программа дисциплины «Программные и программно-аппаратные средства обеспечения информационной безопасности» разработана на основе требований Федерального государственного образовательного стандарта (далее – ФГОС) среднего профессионального образования (СПО) (СПО) по специальности 10.02.05. Обеспечение информационной безопасности автоматизированных систем от 9 декабря 2016 г. № 1553 для реализации основной профессиональной образовательной программы СПО на базе основного общего образования с получением среднего общего образования.

Организация-разработчик: колледж федерального государственного бюджетного образовательного учреждение высшего образования «Дагестанский государственный университет» (Колледж ДГУ)

Разработчики:

Шахбанова М.И. - преподаватель кафедры естественно-научных и гуманитарных дисциплин Колледжа ФГБОУ ВО «Дагестанский государственный университет»
Шахбанова З.И. - к.э.н., доцент кафедры прикладной информатики в экономике факультета информатики и информационных технологий ФГБОУ ВО «Дагестанский государственный университет»

Рабочая программа дисциплины одобрена на заседании кафедры специальных дисциплин Колледжа ДГУ
протокол № 7 от «27» 02 2021г.

Зав. кафедрой _____ /Магомедова А.М./

Рабочая программа дисциплины согласована с учебно-методическим управлением «26» 03 2021г.

Начальник УМУ, д.б.н., проф. _____ Гасангаджиева А.Г.

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Программные и программно-аппаратные средства обеспечения информационной безопасности

1.1. Область применения программы

Рабочая программа дисциплины «Программные и программно-аппаратные средства обеспечения информационной безопасности» является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности СПО 10.02.05.Обеспечение информационной безопасности автоматизированных систем для очного обучения студентов, имеющих основное общее образование, по программе базовой подготовки.

Рабочие программы дисциплин, адаптированные для обучения лиц с ограниченными возможностями здоровья, разрабатываются с учетом конкретных ограничений здоровья лиц, зачисленных в колледж, и утверждаются в установленном порядке.

1.2. Место дисциплины в структуре основной профессиональной образовательной программы:

Учебная дисциплина «Программные и программно-аппаратные средства обеспечения информационной безопасности» относится к профессиональному модулю «Защита информации в автоматизированных системах программами и программно-аппаратными средствами» профессионального цикла ПССЗ.

1.3. Цели и задачи дисциплины – требования к результатам освоения дисциплины

Целью изучения дисциплины «Программные и программно-аппаратные средства обеспечения информационной безопасности» является формирование у студентов знаний и умений по защите компьютерной информации с применением современных программно-аппаратных средств.

Задачами изучения дисциплины являются:

- методы и средства защиты информации в компьютерных системах;
- защитные механизмы, реализованные в средствах защиты компьютерных систем от несанкционированного доступа (НСД);
- современные программно-аппаратные комплексы защиты информации;
- применение средств криптографической защиты информации и средств защиты от НСД для решения задач обеспечения информационной безопасности.

Приобретенные знания и навыки позволят студентам работать в должностях администраторов компьютерных сетей и администраторов безопасности.

Освоение содержания учебной дисциплины «Программные и программно-аппаратные средства обеспечения информационной безопасности» обеспечивает достижение студентами следующих результатов:

Общие компетенции

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 09. Использовать информационные технологии в профессиональной деятельности.

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.

Профессиональные компетенции

ПК 2.1. Осуществлять установку и настройку отдельных программных, 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.

В результате освоения дисциплины обучающийся должен **уметь:**

- применять программно-аппаратные средства обеспечения информационной безопасности;
- диагностировать, устранять отказы и обеспечивать работоспособность программно-аппаратных средств обеспечения информационной безопасности;
- оценивать эффективность применяемых программно-аппаратных средств обеспечения информационной безопасности;
- участвовать в обеспечении учета, обработки, хранения и передачи конфиденциальной информации;
- применять нормативно-правовые акты, нормативно-методические документы по обеспечению информационной безопасности программно-аппаратными средствами;

– использовать криптографические средства и методы защиты информации.

В результате освоения дисциплины обучающийся должен **знать:**

– базовый понятийный аппарат в области информационной безопасности;
– функционирование системы управления средствами безопасности;
– основные типы моделей управления доступом;
– методы и формы применения программно-аппаратных средств обеспечения информационной безопасности;
– особенности применения программно-аппаратных средств обеспечения информационной безопасности в операционных системах, компьютерных сетях , баз данных;
– типовые средства и методы обеспечения информационной безопасности локальных и глобальных вычислительных сетях.

При реализации содержания учебной дисциплины «Программные и программно-аппаратные средства обеспечения информационной безопасности» в пределах освоения ОПОП СПО на базе основного общего образования с получением среднего общего образования учебная нагрузка студентов составляет **95** часов, из них аудиторная (обязательная) учебная нагрузка, включая лекционные и практические занятия **72** часа; внеаудиторная самостоятельная работа студентов **22** часа; консультация 1 час.

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	***Объем часов***
Максимальная учебная нагрузка (всего)	***95***
Обязательная аудиторная учебная нагрузка (всего)	
в том числе:	
теоретическое обучение	*24*
лабораторные работы	
практические занятия (в т.ч. практическая подготовка)	*48*
контрольные работы	
курсовой проект	
консультация	*1*
Самостоятельная работа обучающегося (всего)	*22*
в том числе:	
самостоятельная работа над курсовым проектом	
внеаудиторная самостоятельная работа	
Промежуточная аттестация в форме экзамена	

2.2. Тематический план и содержание дисциплины « Программные и программно-аппаратные средства обеспечения информационной безопасности»

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся, курсовая работ (проект) *(если предусмотрены)*	Объем часов
1	**2**	**3**
Раздел 1. Основные принципы программной и программно-аппаратной защиты информации		
Тема 1.1. Предмет и задачи программно-аппаратной защиты информации	**Содержание учебного материала**	**8**
	Цели, задачи и содержание курса. Основные понятия. Предмет и задачи программно-аппаратной защиты информации. Автоматизированная система. Структура и компоненты АС. Сети ЭВМ. Способы защиты конфиденциальности, целостности и доступности в КС.	*2*
	Практические занятия/ Лабораторные занятия	*4*
	1. Цели, задачи и содержание курса. 2. Основные понятия. 3. Предмет и задачи программно-аппаратной защиты информации. 4. Автоматизированная система. 5. Структура и компоненты АС. Сети ЭВМ. 6. Способы защиты конфиденциальности, целостности и доступности в КС.	
	Консультации	
	Самостоятельная работа обучающихся: Тестирование, устный опрос.	*2*
Тема 1.2. Проблема защиты программного	**Содержание учебного материала**	**8**
	Проблема защиты программного обеспечения информационных систем. Объекты защиты. Жизненный цикл программного обеспечения	*2*

обеспечения информационных систем	информационных систем. Технологическая и эксплуатационная безопасность программного обеспечения. Основные принципы обеспечения безопасности программного обеспечения. Защита программного обеспечения как система научных дисциплин. Уязвимости программного обеспечения. Угрозы безопасности программного обеспечения. Вредоносные программы. Несанкционированные исследование и копирование программ.	
	Практические занятия/ Лабораторные занятия	*4*
	1. Проблема защиты программного обеспечения информационных систем. 2. Объекты защиты. 3. Жизненный цикл программного обеспечения информационных систем. 4. Технологическая и эксплуатационная безопасность программного обеспечения. 5. Основные принципы обеспечения безопасности программного обеспечения. 6. Защита программного обеспечения как система научных дисциплин. 7. Уязвимости программного обеспечения. 8. Угрозы безопасности программного обеспечения. 9. Вредоносные программы. 10. Несанкционированные исследование и копирование программ.	
	Консультации	
	Самостоятельная работа обучающихся: Тестирование, устный опрос.	*2*
Тема 1.3. Стандарты безопасности	**Содержание учебного материала**	**8**
	Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Профили защиты программных и программно-аппаратных средств (межсетевых экранов,	*2*

	средств контроля съемных машинных носителей информации, средств доверенной загрузки, средств антивирусной защиты). Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.	
	Практические занятия/ Лабораторные занятия	*4*
	1. Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. 2. Профили защиты программных и программно-аппаратных средств (межсетевых экранов, средств контроля съемных машинных носителей информации, средств доверенной загрузки, средств антивирусной защиты). 3. Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. 4. Обзор нормативных правовых актов, нормативных методических документов по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. 5. Работа с содержанием нормативных правовых актов.	
	Консультации	
	Самостоятельная работа обучающихся: Тестирование, устный опрос. Подготовка доклада.	*2*
Тема 1.4. Защищенная автоматизированная система	**Содержание учебного материала**	**8**
	Автоматизация процесса обработки информации. Понятие автоматизированной системы. Особенности автоматизированных систем в защищенном исполнении. Основные виды АС в защищенном исполнении. Методы создания безопасных систем. Методология проектирования	*2*

	гарантированно защищенных КС Дискреционные модели. Мандатные модели.	
	Практические занятия/ Лабораторные занятия:	*4*
	1. Автоматизация процесса обработки информации. 2. Понятие автоматизированной системы. 3. . Особенности автоматизированных систем в защищенном исполнении. 4. Основные виды АС в защищенном исполнении. Методы создания безопасных систем. 5. Методология проектирования гарантированно защищенных КС Дискреционные модели Мандатные модели. 6. Учет, обработка, хранение и передача информации в АИС 7. Ограничение доступа на вход в систему. 8. Идентификация и аутентификация пользователей 9. Разграничение доступа. 10. Регистрация событий (аудит). 11. Контроль целостности данных 12. Уничтожение остаточной информации. 13. Управление политикой безопасности. Шаблоны безопасности 14. Криптографическая защита. Обзор программ шифрования данных. 15. Управление политикой безопасности. Шаблоны безопасности	
	Консультации	
	Самостоятельная работа обучающихся: Тестирование, устный опрос	*2*
Тема 1.5. Принципы программно-аппаратной защиты информации от несанкционированно	**Содержание учебного материала**	**8**
	Понятие несанкционированного доступа к информации. Основные подходы к защите информации от НСД. Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам. Доступ к данным со стороны процесса. Особенности защиты данных от изменения. Шифрование.	*2*

го доступа	**Практические занятия/ Лабораторные занятия:**	*4*
	1. Организация доступа к файлам. 2. Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД. 3. Понятие несанкционированного доступа к информации. 4. Основные подходы к защите информации от НСД. 5. Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам. 6. Доступ к данным со стороны процесса Особенности защиты данных от изменения. Шифрование.	
	Консультации	
	Самостоятельная работа обучающихся: Доклад, разработка презентации к докладу на семинаре, поиск информации в сетях.	*2*
Раздел 2. Защита информации в локальных сетях		
Тема 2.1. Основы построения защищенных сетей	**Содержание учебного материала**	**8**
	Сети, работающие по технологии коммутации пакетов 14 Стек протоколов TCP/IP. Особенности маршрутизации. Штатные средства защиты информации стека протоколов TCP/IP. Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения.	*2*
	Практические занятия/ Лабораторные занятия:	*4*
	1. Сети, работающие по технологии коммутации пакетов. 2. Стек протоколов TCP/IP. Особенности маршрутизации. 3. Штатные средства защиты информации стека протоколов TCP/IP. 4. Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения. 5. Виртуальная частная сеть.	

	6. Функции, назначение, принцип построения.	
	Консультации	
	Самостоятельная внеаудиторная работа: Подготовить сообщение по теме: Коммуникационное оборудование. Технология локальных сетей.	*2*
Тема 2.2. Средства организации VPN	**Содержание учебного материала**	**8**
	Виртуальная частная сеть. Функции, назначение, принцип построения 10 Криптографические и некриптографические средства организации VPN. Устройства, образующие VPN. Криптомаршрутизатор и криптофильтр. Криптороутер. Принципы, архитектура, модель нарушителя, достоинства и недостатки Криптофильтр. Принципы, архитектура, модель нарушителя, достоинства и недостатки.	*2*
	Практические занятия/ Лабораторные занятия:	*4*
	1. Виртуальная частная сеть. Функции, назначение, принцип построения. 2. Криптографические и некриптографические средства организации VPN. 3. Устройства, образующие VPN. Криптомаршрутизатор и криптофильтр. 4. Криптороутер. Принципы, архитектура, модель нарушителя, достоинства и недостатки. 5. Криптофильтр. Принципы, архитектура, модель нарушителя, достоинства и недостатки.	
	Консультации	
	Самостоятельная внеаудиторная работа: Подготовить сообщение по теме: Коммуникационное оборудование. Технология локальных сетей.	*2*
Тема 2.3. Обеспечение безопасности	**Содержание учебного материала**	**8**
	Методы защиты информации при работе в сетях общего доступа. Межсетевые экраны типа firewall. Достоинства, недостатки, реализуемые	*2*

межсетевого взаимодействия	политики безопасности Основные типы firewall. Симметричные и несимметричные firewall. Уровень 1. Пакетные фильтры Уровень 2. Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне. Уровень 3.	
	Практические занятия/ Лабораторные занятия:	*4*
	1. Методы защиты информации при работе в сетях общего доступа. 16 Межсетевые экраны типа firewall. 2. Достоинства, недостатки, реализуемые политики безопасности Основные типы firewall. 3. Симметричные и несимметричные firewall. Уровень 1. Пакетные фильтры Уровень 2. 4. Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне. Уровень 3. 5. Proxy-сервера прикладного уровня. 6. Однохостовые и мультихостовые firewall. 7. Основные типы архитектур мультихостовых firewall. 8. Требования к каждому хосту исходя из архитектуры и выполняемых функций. 9. Требования по сертификации межсетевых экранов	
	Консультации	
	Самостоятельная внеаудиторная работа: Подготовить доклад по теме.	*2*
Тема 2.4. Исследование программного обеспечения на предмет отсутствия недекларированных возможностей	**Содержание учебного материала**	**8**
	Сертификация средств защиты информации по требованиям безопасности информации. Проверка соответствия реальных и декларируемых функциональных возможностей. Проверка отсутствия недекларируемых возможностей. Методы проведения испытаний. Документация, представляемая на испытания. Статический анализ исходных текстов и исполняемых модулей ПО.	*2*

	Контроль полноты и отсутствия избыточности исходных текстов на уровне файлов. Контроль соответствия исходных текстов ПО его объектному (загрузочному) коду. Контроль связей функциональных объектов по управлению и информации. Синтаксический контроль наличия заданных конструкций. Формирование и анализ маршрутов выполнения функциональных объектов.	
	Практические занятия/ Лабораторные занятия:	*4*
	1. Сертификация средств защиты информации по требованиям безопасности информации. 2. Проверка соответствия реальных и декларируемых функциональных возможностей. Проверка отсутствия недекларируемых возможностей. 3. Методы проведения испытаний. Документация, представляемая на испытания. 4. Статический анализ исходных текстов и исполняемых модулей ПО. 5. Контроль полноты и отсутствия избыточности исходных текстов на уровне файлов. 6. Контроль соответствия исходных текстов ПО его объектному (загрузочному) коду. 7. Контроль связей функциональных объектов по управлению и информации. 8. Синтаксический контроль наличия заданных конструкций. 9. Формирование и анализ маршрутов выполнения функциональных объектов.	
	Консультации	
	Самостоятельная внеаудиторная работа: Подготовить доклад по теме.	*2*
Раздел 4. Мониторинг систем защиты		
Тема 4.1.	**Содержание учебного материала**	**8**

Мониторинг систем защиты	Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации. Особенности фиксации событий, построенных на разных принципах: сети с коммутацией соединений, сеть с коммутацией пакетов, TCP/IP, X.25. Классификация отслеживаемых событий. Особенности построения систем мониторинга Источники информации для мониторинга: сетевые мониторы, статистические характеристики трафика через МЭ, проверка ресурсов общего пользования. Классификация сетевых мониторов. Системы управления событиями информационной безопасности (SIEM). Обзор SIEM-систем на мировом и российском рынке.	*2*
	Практические занятия/ Лабораторные занятия:	*4*
	1. Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации. 2. Особенности фиксации событий, построенных на разных принципах: сети с коммутацией соединений, сеть с коммутацией пакетов, TCP/IP, X.25. 3. Классификация отслеживаемых событий. 4. Особенности построения систем мониторинга. 5. Источники информации для мониторинга: сетевые мониторы, статистические характеристики трафика через МЭ, проверка ресурсов общего пользования. 6. Классификация сетевых мониторов. 7. Системы управления событиями информационной безопасности (SIEM). 8. Обзор SIEM-систем на мировом и российском рынке.	
	Консультации	
	Самостоятельная внеаудиторная работа: Работа с учебной литературой, выполнение домашнего задания.	*2*
Тема 4.2. Изучение	**Содержание учебного материала**	**7**
	Изучение требований о защите информации, не составляющей	*2*

современных программно-аппаратных комплексов.	государственную тайну. Изучение методических документов ФСТЭК по применению мер защиты. Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов Установка и настройка программных средств оценки защищенности и аудита информационной безопасности, изучение функций и настройка режимов работы на примере MaxPatrol или других аналогов Изучение функционала и областей применения DLP систем на примере nfoWatchTrafficMonitor или других аналогов.	
	Практические занятия/ Лабораторные занятия:	*4*
	1. Изучение требований о защите информации, не составляющей государственную тайну. 2. Изучение методических документов ФСТЭК по применению мер защиты. 3. Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов 4. Установка и настройка программных средств оценки защищенности и аудита информационной безопасности, изучение функций и настройка режимов работы на примере MaxPatrol или других аналогов. 5. Изучение типовых решений для построения VPN на примере VipNet или других аналогов. 6. Изучение современных систем антивирусной защиты на примере корпоративных решений KasperskyLab или других аналогов. 7. Изучение функционала и областей применения DLP систем на примере InfoWatchTrafficMonitor или других аналогов.	
	Консультации	

	Самостоятельная внеаудиторная работа: Работа с конспектом лекций, подготовка к практическим занятиям, подготовка к комбинированному опросу.	*1*
Тема 4.3. **Методы обеспечения технологической и эксплуатационной безопасности программного обеспечения**	**Содержание учебного материала**	**8**
	Классификация вредоносных программ. Защита от вредоносных программ Методы тестирования программного обеспечения на его защищенность. Методы тестирования программ. Фаззинг программ. Методы защиты программ от несанкционированного исследования. Классификация средств несанкционированного исследования программ. Способы защиты программ от несанкционированного исследования. Обфускация программ. Способы встраивания защитных механизмов в программное обеспечение. Методы защиты программ от несанкционированного копирования. Криптографические методы защиты от копирования. Метод привязки к идентификатору. Методы, основанные на работе с переходами и стеком. Манипуляции с кодом программы. Методы противодействия динамическим способам снятия защиты программ от копирования.	*2*
	Практические занятия/ Лабораторные занятия:	*4*
	1. Классификация вредоносных программ. 2. Защита от вредоносных программ. 3. Методы тестирования программного обеспечения на его защищенность. 4. Методы тестирования программ. 5. Фаззинг программ. 6. Методы защиты программ от несанкционированного исследования. 7. Классификация средств несанкционированного исследования программ. 8. Способы защиты программ от несанкционированного исследования. 9. Обфускация программ. Способы встраивания защитных механизмов в	

	программное обеспечение. 10. Методы защиты программ от несанкционированного копирования. Криптографические методы защиты от копирования. 11. Метод привязки к идентификатору. Методы, основанные на работе с переходами и стеком. 12. Манипуляции с кодом программы. 13. Методы противодействия динамическим способам снятия защиты программ от копирования.	
	Консультации	*1*
	Самостоятельная внеаудиторная работа: Работа с конспектом лекций, подготовка к практическим занятиям, подготовка к комбинированному опросу.	*1*
Примерная тематика курсовой работы (проекта) *(если предусмотрены)*		*не предусмотрено*
Самостоятельная работа обучающихся над курсовой работой (проектом) *(если предусмотрены)*		*не предусмотрено*
	Всего:	***95***

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Учебная аудитория для проведения лекционных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Оснащение аудитории:

- комплект учебной мебели: парты, стол преподавательский, стулья, доска;
- мультимедийная система: проектор, экран настенный, ноутбук.

Программное обеспечение ноутбука лекционных аудиторий:

- лицензионное программное обеспечение:
- ОС Microsoft Windows;
- свободно распространяемое программное обеспечение:
- офисный пакет LibreOffice;
- программа просмотра pdf-документов Sumatra PDF Reader.

Практические занятия проводятся в кабинете интернет-технологий и информатики, оборудованным ПЭВМ с установленным программным обеспечением:

- лицензионное программное обеспечение:
- ОС Microsoft Windows;
- свободно распространяемое программное обеспечение:
- офисный пакет LibreOffice;
- система программирования «Microsoft Visual Studio Express»;
- программа просмотра pdf-документов Sumatra PDF Reader.

Для самостоятельной работы студентов используется кабинет интернет-технологий и информатики.
Оснащение кабинета:

- комплект учебной мебели: стол преподавательский, столы компьютерные, стулья
- персональные компьютеры, сетевой коммутатор, сетевая кабельная система.

Программное обеспечение:

- лицензионное программное обеспечение:
- ОС Microsoft Windows
- Антивирус Касперского
- свободно распространяемое программное обеспечение:
- офисный пакет LibreOffice;
- Windows 10
- Microsoft Office Professional
- Adobe Acrobat Reader DC

- VLC Media player
- 7-zip
- ПАК Соболь
- МДЗ-Эшелон
- Dallas Lock 8.0-K
- «ФИКС» 10.
- «Terrier-2.0»
- «Ревизор-1 XP»
- «Ревизор-2 XP»
- Kaspersky Endpoint Security 11
- программа просмотра pdf-документов Sumatra PDF Reader.

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основная литература:

1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2021. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/476997
2. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/449548

Дополнительная литература:

1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2019. — 312 с. — (Специалист). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/
2. Долозов Н. Л., Гультяева Т. А. Программные средства защиты информации: конспект лекций Новосибирск: Новосибирский государственный технический университет, 2015. – 63 с. https://biblioclub.ru/index.php?page=book_red&id=438307&sr=1
3. Ю.Ю. Громов, О.Г. Иванова, К.В. Стародубов, А.А. Кадыков Программно-аппаратные средства защиты информационных систем :

учебное пособие Тамбов : Издательство ФГБОУ ВПО «ТГТУ», 2017. – 194 с. https://biblioclub.ru/index.php?page=book_red&id=499013&sr=1
4. Рецензируемый научный журнал «Проблемы информационной безопасности».
5. Научный журнал «Прикладная дискретная математика»
6. Научный журнал «Информатика и ее применение»
7. Журнал о компьютерах и цифровой технике «ComputerBild»
8. Рецензируемый научный журнал «Информатика и система управления»
9. Рецензируемый научный журнал «Проблемы информационной безопасности»
10. Рецензируемый научный журнал «Прикладная информатика»
11. Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями и дополнениями).
12. ГОСТ 34.320-96.Информационные технологии. Система стандартов по базам данных. Концепции и терминология для концептуальной схемы и информационной базы. 2001 г.www.standartgost.ru
13. ГОСТ Р ИСО/МЭК ТО 12182-2002. Информационная технология. Классификация программных средств. 2002 г.www.standartgost.ru
14. ГОСТ Р ИСО/МЭК 15288-2005. Информационная технология. Системная инженерия. Процессы жизненного цикла систем. 2006 г.www.standartgost.ru
15. ГОСТ Р ИСО/МЭК 12119-2000. Информационная технология. Пакеты программ. Требования к качеству и тестирование. 2005 г.www.standartgost.ru
16. ГОСТ 34.601-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания. 2009 г.www.standartgost.ru
17. ГОСТ 28195-89. Оценка качества программных средств. Общие положения. 2001 г.www.standartgost.ru
18. ГОСТ 34.602-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.www.standartgost.ru

Интернет-ресурсы:

1. Научная электронная библиотека eLIBRARY.RU [Электронный ресурс]. URL: http://elibrary.ru
2. Национальная электронная библиотека [Электронный ресурс]. URL: https://нэб.рф/.
3. Электронно-библиотечная система «Университетская библиотека онлайн» [Электронный ресурс]. URL: http://biblioclub.ru
4. Официальный сайт компании «Консультант Плюс» URL: http://www.consultant.ru
5. Справочная правовая система «Гарант». URL: http://www.garant.ru

6. Информационные ресурсы научной библиотеки Даггосуниверситета [Электронный ресурс]. URL: http://elib.dgu.ru.
7. Юридический вестник ДГУ. URL: www.jurvestnik.dgu.ru
8. Федеральный портал «Российское образование» [Электронный ресурс]. URL: http://www.edu.ru
9. Электронно-библиотечная система Юрайт [Электронный ресурс]. URL: https://urait.ru/.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

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

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
В результате освоения дисциплины обучающийся должен **уметь:** – формулировать требования к подсистеме защиты информации и к ее программно-аппаратным компонентам; – проектировать подсистему защиты информации в автоматизированной системе в части ее программно-аппаратных компонент защиты от несанкционированного доступа к информации, защиты от несанкционированного копирования информации, подсистем идентификации и аутентификации, защиты от разрушающих программных воздействий и защиты программного обеспечения от изучения; – обосновывать необходимость применения тех или иных программно-аппаратных средств обеспечения информационной безопасности; обосновывать необходимость применения тех или иных программно-аппаратных средств обеспечения информационной безопасности; – работать с программно-аппаратными	Комбинированный метод контроля в форме индивидуального, фронтального опроса и самостоятельной работы; тестирование; рефераты; составление и оформление письменных документов; подготовка и защита рефератов; экспертная оценка результатов выполнения индивидуальных практических работ по решению ситуационных задач.

комплексами защиты информации: Secret Net 4.0, Dallas Lock 7.0 и Secret Disk.	
В результате освоения дисциплины обучающийся должен **знать:** – основы построения политики безопасности для различных систем; – как защитить ПЭВМ от локального несанкционированного доступа, как применять различные схемы идентификации и аутентификации, как защищать программы от несанкционированного копирования с помощью ключей; – как защитить КС от различных типов разрушающих программных воздействий, в том числе файловых вирусов, загрузочных вирусов, программ типа «троянский конь»;. – как осуществлять регламентные работы, связанные с комплексным обеспечением информационной безопасности конкретных автоматизированных систем, и работ, осуществляемых в режимах нештатных ситуаций, в том числе мероприятий, - обязательных для автоматизированных систем, содержащих сведения, составляющие государственную тайну; - как обеспечить эффективное использование средств автоматического контроля, обнаружения и закрытия возможных каналов утечки конфиденциальных сведений;	Интерпретация результатов устного опроса; текущий контроль в форме тестирования; текущий контроль усвоения материала в форме комбинированного опроса; экспертная оценка результатов выполнения домашнего задания; текущий контроль в форме комбинированного опроса; экспертная оценка результатов выполнения домашнего задания.