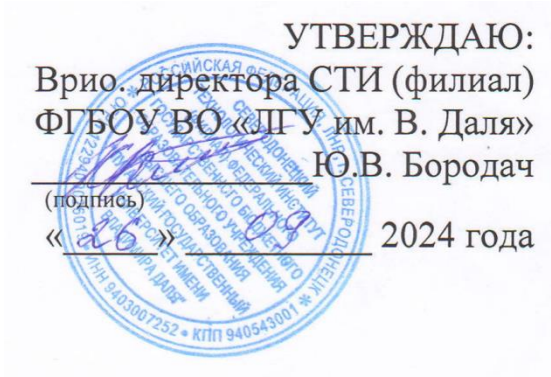
МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Луганский государственный университет имени Владимира Даля»
(ФГБОУ ВО «ЛГУ им. В. Даля»)

Северодонецкий технологический институт
Кафедра информационных технологий, приборостроения и электротехники



РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«Комплексное обеспечение информационной безопасности»

По направлению подготовки: 09.04.01 Информатика и вычислительная техника

Магистерская программа «Цифровые технологии в экономике»

Северодонецк – 2024

Лист согласования РПУД

Рабочая программа учебной дисциплины «Комплексное обеспечение информационной безопасности» по направлению подготовки 09.04.01 Информатика и вычислительная техника (магистерская программа «Цифровые технологии в экономике») – 24 с.

Рабочая программа учебной дисциплины «Комплексное обеспечение информационной безопасности» разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования – магистратура по направлению подготовки 09.04.01 Информатика и вычислительная техника, утвержденным приказом Министерства образования и науки Российской Федерации от 19 сентября 2017 г. № 918 (с изменениями и дополнениями в соответствии с приказами Министерства образования и науки Российской Федерации № 1456 от 26.11.2020 г., № 82 от 08.02.2021 г.).

СОСТАВИТЕЛЬ:
ст. преподаватель Е.В. Кузнецова

Рабочая программа дисциплины утверждена на заседании кафедры информационных технологий, приборостроения и электротехники «_05_» _____09____ 2024 г., протокол №_1_.

Заведующий кафедрой ИТПЭ _____ В.Г. Чебан

Переутверждена: «_____» _____ 202___ г., протокол №_____.

Рекомендована на заседании учебно-методической комиссии Северодонецкого технологического института (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Луганский государственный университет имени Владимира Даля» «_16_» ____09_____ 2024 г., протокол №_1_.

Председатель учебно-методической комиссии
СТИ (филиал) ФГБОУ ВО «ЛГУ им. В. Даля» _____ Ю.В. Бородач

1. Цели и задачи освоения дисциплины

Цель изучения дисциплины – формирование системы теоретических знаний и практических навыков в области комплексного обеспечения информационной безопасности; определение места информационной безопасности в национальной безопасности страны; усвоение достижений науки и практики в области анализа и классификации угроз безопасности информации, мер противодействия данным угрозам.

Задачи:

- изучение основных понятий, теоретических основ и принципов комплексного обеспечения информационной безопасности;
- формирование умений решения задач по обеспечению информационной безопасности на законодательном, административном, процедурном, программно-техническом уровнях.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Комплексное обеспечение информационной безопасности» входит в обязательную часть дисциплин учебного плана.

Необходимыми условиями для освоения дисциплины являются:

знания: различных подходов к определению понятия "информационная безопасность"; определений конфиденциальности и доступности информации; задач информационной безопасности; уровней формирования режима информационной безопасности; характерных черт компьютерных вирусов и защита от них; механизмов идентификации и аутентификации;

умения: распределять задачи информационной безопасности по уровням ее обеспечения; использовать механизмы идентификации и аутентификации для защиты информационных технологий; использовать методы разграничения доступа;

навыки: владения механизмами обеспечения информационной безопасности.

Содержание дисциплины является логическим продолжением содержания дисциплин: «ERP-системы», «Автоматизированные системы обработки информации и управления», «Управление рисками в профессиональной деятельности».

Служит основой для прохождения преддипломной (производственной) практики, для выполнения и защиты выпускной квалификационной работы.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

Код и наименование компетенции	Индикаторы достижений компетенции (по реализуемой дисциплине)	Перечень планируемых результатов
ОПК-5. Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем	ОПК-5.1. Знает современное программное и аппаратное обеспечение информационных и автоматизированных систем ОПК-5.2. Умеет разрабатывать программное и аппаратное обеспечение информационных и автоматизированных систем для решения профессиональных задач ОПК-5.3. Владеет навыками разработки программного и аппаратного обеспечения информационных и автоматизированных систем для решения профессиональных задач	**Знать:** современное программное и аппаратное обеспечение информационных и автоматизированных систем **Уметь:** разрабатывать программное и аппаратное обеспечение информационных и автоматизированных систем для решения профессиональных задач **Владеть:** навыками разработки программного и аппаратного обеспечения информационных и автоматизированных систем для решения профессиональных задач

ОПК-6. Способен разрабатывать компоненты программно-аппаратных комплексов обработки информации и автоматизированного проектирования	ОПК-6.1. Знает аппаратные средства и платформы инфраструктуры информационных технологий, виды, назначение, архитектуру, методы разработки и администрирования программно-аппаратных комплексов объекта профессиональной деятельности ОПК-6.2. Умеет анализировать техническое задание, разрабатывать и оптимизировать программный код для решения задач обработки информации и автоматизированного проектирования ОПК-6.3. Владеет методами составления технической документации по использованию и настройке компонентов программно-аппаратного комплекса	**Знать:** аппаратные средства и платформы инфраструктуры информационных технологий, виды, назначение, архитектуру, методы разработки и администрирования программно-аппаратных комплексов объекта профессиональной деятельности **Уметь:** анализировать техническое задание, разрабатывать и оптимизировать программный код для решения задач обработки информации и автоматизированного проектирования **Владеть:** методами составления технической документации по использованию и настройке компонентов программно-аппаратного комплекса
ПК-2. Способен осуществлять проектирование защищенных информационных систем	ПК-2.1. Знает нормативную базу, методы описания, анализа и проектирования в области обеспечения безопасности информационных систем ПК-2.2. Умеет выбирать методы и средства проектирования защищенных информационных систем ПК-2.3. Владеет навыками разработки аппаратных и программных средств, необходимых для обеспечения безопасности информационных систем	**Знать:** нормативную базу, методы описания, анализа и проектирования в области обеспечения безопасности **Уметь:** выбирать методы и средства проектирования защищенных информационных систем **Владеть:** навыками разработки аппаратных и программных средств, необходимых для обеспечения безопасности информационных систем

4. Структура и содержание дисциплины

4.1. Объём учебной дисциплины и виды учебной работы

Вид учебной работы	Объём часов (зач. ед.)	
	Очная форма	**Заочная форма**
Общая учебная нагрузка (всего)	180 (5 зач. ед)	180 (5 зач. ед)
Обязательная аудиторная учебная нагрузка (всего) в том числе:	96	48
Лекции	48	24
Семинарские занятия	-	-
Практические занятия	48	24
Лабораторные работы	-	-
Курсовая работа (курсовой проект)	-	-
Другие формы и методы организации образовательного процесса (*индивидуальные задания)*	27	36
Самостоятельная работа студента (всего)	57	96
Форма аттестации	экзамен	экзамен

4.2. Содержание разделов дисциплины

Тема 1. Информационная безопасность и уровни ее обеспечения.

Понятие "информационная безопасность". Составляющие информационной безопасности. Система формирования режима информационной безопасности. Уровни формирования режима информационной безопасности. Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации.

Тема 2. Стандарты информационной безопасности: "Общие критерии".

Требования безопасности к информационным системам Принцип иерархии: класс – семейство – компонент – элемент. Функциональные требования. Требования доверия.

Тема 3. Стандарты информационной безопасности распределенных систем.

Сервисы безопасности в вычислительных сетях. Механизмы безопасности. Администрирование средств безопасности.

Тема 4. Классификация угроз "информационной безопасности".

Классы угроз информационной безопасности. Каналы несанкционированного доступа к информации.

Тема 5. Компьютерные вирусы и защита от них.

Вирусы как угроза информационной безопасности. Характерные черты компьютерных вирусов.

Тема 6. Классификация компьютерных вирусов.

Классификация компьютерных вирусов по среде обитания. Классификация компьютерных вирусов по особенностям алгоритма работы. Классификация компьютерных вирусов по деструктивным возможностям.

Тема 7. Характеристика "вирусоподобных" программ.

Виды "вирусоподобных" программ. Характеристика "вирусоподобных" программ. Утилиты скрытого администрирования. "Intended"-вирусы.

Тема 8. Антивирусные программы.

Особенности работы антивирусных программ. Классификация антивирусных программ. Факторы, определяющие качество антивирусных программ. Профилактика компьютерных вирусов.

Тема 9. Механизмы обеспечения "информационной безопасности".

Идентификация и аутентификация. Определение понятий "идентификация" и "аутентификация". Механизм идентификация и аутентификация пользователей.

Тема 10. Криптография и шифрование.

Структура криптосистемы. Классификация систем шифрования данных. Симметричные и асимметричные методы шифрования. Механизм электронной цифровой подписи.

4.3. Лекции

№ п/п	Название темы	Объём часов	
		Очная форма	Заочная форма
1.	Информационная безопасность и уровни ее обеспечения	4	2
2.	Стандарты информационной безопасности: "Общие критерии"	4	2
3.	Стандарты информационной безопасности распределенных систем	8	4
4.	Классификация угроз "информационной безопасности"	8	4
5.	Компьютерные вирусы и защита от них	4	2
6.	Классификация компьютерных вирусов	4	2
7.	Характеристика "вирусоподобных" программ	4	2
8.	Антивирусные программы	4	2
9.	Механизмы обеспечения "информационной безопасности"	4	2
10.	Криптография и шифрование	4	2
Итого:		**48**	**24**

4.4. Практические (семинарские) занятия

№ п/п	Название темы	Объём часов	
		Очная форма	Заочная форма
1.	Виды информации и основные методы ее защиты	2	2
2.	Виды угроз информационной безопасности	2	
3.	Источники угроз информационной безопасности	2	2
4.	Анализ информационной инфраструктуры государства	2	
5.	Исследование атаки переполнения буфера как примера нарушения конфиденциальности, целостности и доступности информации	2	2
6.	Причины, виды, каналы утечки и искажения информации	2	
7.	Технические средства и методы защиты информации	2	2
8.	Программно-аппаратные средства обеспечения информационной безопасности	2	
9.	Тестовые испытания программных средств защиты	4	4
10.	Защита от утечек по каналу ПЭМИН, по акустическому и виброакустическому каналам	4	
11.	Анализ сетевой топологии и установленных сервисов	4	4
12.	Сетевое сканирование	4	

13.	Анализ трафика и сбор критичной информации программами пассивного анализа	4	4
14.	Обнаружение уязвимостей по сигнатурам	4	
15.	Оценка уязвимости коммутируемого доступа	4	4
16.	Аудит комплексной защиты информации предприятия	4	
Итого:		**48**	**24**

4.5. Лабораторные работы

Лабораторные работы по дисциплине «Комплексное обеспечение информационной безопасности» не предусмотрены учебным планом.

4.6. Самостоятельная работа студентов

№ п/п	Название темы	Вид СРС	Объем часов	
			Очная форма	Заочная форма
1.	Информационная безопасность и уровни ее обеспечения	Изучение лекционного материала. Подготовка к практическим занятиям.	5	9
2.	Стандарты информационной безопасности: "Общие критерии"	Изучение лекционного материала. Подготовка к практическим занятиям.	6	10
3.	Стандарты информационной безопасности распределенных систем	Изучение лекционного материала. Подготовка к практическим занятиям.	6	10
4.	Классификация угроз "информационной безопасности"	Изучение лекционного материала. Подготовка к практическим занятиям.	5	9
5.	Компьютерные вирусы и защита от них	Изучение лекционного материала. Подготовка к практическим занятиям.	5	9
6.	Классификация компьютерных вирусов	Изучение лекционного материала. Подготовка к практическим занятиям.	6	9
7.	Характеристика "вирусоподобных" программ	Изучение лекционного материала. Подготовка к практическим занятиям.	6	10
8.	Антивирусные программы	Изучение лекционного материала. Подготовка к практическим занятиям.	6	10
9.	Механизмы обеспечения "информационной безопасности"	Изучение лекционного материала. Подготовка к практическим занятиям.	6	10
10.	Криптография и шифрование	Изучение лекционного материала. Подготовка к практическим занятиям.	6	10
Итого:			**57**	**96**

4.7. Курсовые работы/проекты

Курсовые работы (проекты) по данной дисциплине не предусмотрены учебным планом.

5. Образовательные технологии

Преподавание дисциплины ведётся с применением следующих видов образовательных технологий:

- традиционные объяснительно-иллюстративные технологии, которые обеспечивают доступность учебного материала для большинства студентов, системность, отработанность организационных форм и привычных методов, относительно малые затраты времени;
- технологии проблемного обучения, направленные на развитие познавательной активности, творческой самостоятельности студентов и предполагающие последовательное и целенаправленное выдвижение перед студентом познавательных задач, разрешение которых позволяет студентам активно усваивать знания (используются поисковые методы, постановка познавательных задач);
- технологии развивающего обучения, позволяющие ориентировать учебный процесс на потенциальные возможности студентов, их реализацию и развитие;
- технологии концентрированного обучения, суть которых состоит в создании максимально близкой к естественным психологическим особенностям человеческого восприятия структуры учебного процесса, и которые дают возможность глубокого и системного изучения содержания учебных дисциплин за счёт объединения занятий в тематические блоки;
- технологии модульного обучения, дающие возможность обеспечения гибкости процесса обучения, адаптации его к индивидуальным потребностям и особенностям обучающихся (применяются, как правило, при самостоятельном обучении студентов по индивидуальному учебному плану);
- технологии дифференцированного обучения, обеспечивающие возможность создания оптимальных условий для развития интересов и способностей студентов, в том числе и студентов с особыми образовательными потребностями, что позволяет реализовать в культурно-образовательном пространстве университета идею создания равных возможностей для получения образования;
- технологии активного (контекстного) обучения, с помощью которых осуществляется моделирование предметного, проблемного и социального содержания будущей профессиональной деятельности студентов (используются активные и интерактивные методы обучения) и т.д.

Максимальная эффективность педагогического процесса достигается путём конструирования оптимального комплекса педагогических технологий и (или) их элементов на личностно-ориентированной, деятельностной, диалогической основе и использования необходимых современных средств обучения.

6. Учебно-методическое и информационное обеспечение дисциплины

а) Основная литература:

1. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. – М. : Риор, 2018. – 400 с.

2. Электронное издание на основе: Информационная безопасность и защита информации. – М. : ДМК Пресс, 2014. – 702 с.: ил. – ISBN 978-5-94074-768-0.

3. Глинская, Е.В. Информационная безопасность конструкций ЭВМ и систем: Учебное пособие / Е.В. Глинская, Н.В. Чичварин. – М. : Инфра-М, 2018. - 64 с.

б) Дополнительная литература:

1. Бабаш, А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. – М.: КноРус, 2019. – 432 с.

2. Бирюков, А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. – М.: ДМК Пресс, 2013. – 474 с.

3. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. – Рн/Д: Феникс, 2010. – 324 с.

4. Гришина, Н.В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. – М. : Форум, 2018. – 118 с.

5. Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. – М. : Форум, 2018. – 88 с.

6. Семененко, В.А. Информационная безопасность / В.А. Семененко. – М. : МГИУ, 2011. – 277 с.

в) Интернет-ресурсы:

1. Министерство образования и науки Российской Федерации – http://минобрнауки.рф
2. Министерства природных ресурсов и экологии Российской Федерации – http://www.mnr.gov.ru
3. Федеральная служба по надзору в сфере образования и науки – http://obrnadzor.gov.ru
4. Министерство образования и науки Луганской Народной Республики – https://minobr.su
5. Министерство природных ресурсов и экологической безопасности ЛНР – https://www.mprlnr.su
6. Народный совет Луганской Народной Республики – https://nslnr.su
7. Портал Федеральных государственных образовательных стандартов высшего образования – http://fgosvo.ru
8. Федеральный портал «Российское образование» – http://www.edu.ru
9. Информационная система «Единое окно доступа к образовательным ресурсам» – http://window.edu.ru
10. Федеральный центр информационно-образовательных ресурсов – http://fcior.edu.ru

Электронные библиотечные системы и ресурсы:

1. Электронно-библиотечная система «Консультант студента» – http://www.studentlibrary.ru/cgi-bin/mb4x
2. Электронно-библиотечная система «StudMed.ru» – https://www.studmed.ru
3. Научная электронная библиотека eLIBRARI.RU» – http://elibrary.ru
4. ЭБС Издательства «ЛАНЬ» – https://e.lanbook.com

Информационный ресурс библиотеки образовательной организации

1. Научная библиотека имени А. Н. Коняева – http://biblio.dahluniver.ru

7. Материально-техническое обеспечение дисциплины

Освоение дисциплины «Комплексное обеспечение информационной безопасности» предполагает использование академических аудиторий, соответствующих действующим санитарным и противопожарным правилам и нормам.

Лекционные занятия: комплект электронных презентаций/слайдов; аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук).

Практические занятия: учебный компьютерный класс, имеющий рабочие места студентов, оснащённые компьютерами с доступом в Интернет, презентационная техника (проектор, экран, компьютер/ноутбук), бесплатное программное обеспечение.

Прочее: рабочее место преподавателя, оснащённое компьютером с доступом в Интернет. В качестве материально-технического обеспечения дисциплины могут быть использованы мультимедийные средства; наборы слайдов, демонстрационные приборы, при необходимости – средства мониторинга и т.д.

Программное обеспечение:

Функциональное назначение	**Бесплатное программное обеспечение**	**Ссылки**
Офисный пакет	Libre Office 6.3.1	https://www.libreoffice.org/ https://ru.wikipedia.org/wiki/LibreOffice
Операционная система	UBUNTU 19.04	https://ubuntu.com/ https://ru.wikipedia.org/wiki/Ubuntu
Браузер	Firefox Mozilla	http://www.mozilla.org/ru/firefox/fx
Браузер	Opera	http://www.opera.com
Почтовый клиент	Mozilla Thunderbird	http://www.mozilla.org/ru/thunderbird
Файл-менеджер	Far Manager	http://www.farmanager.com/download.php
Архиватор	7Zip	http://www.7-zip.org/
Графический редактор	GIMP (GNU Image Manipulation Program)	http://www.gimp.org/ http://gimp.ru/viewpage.php?page_id=8 http://ru.wikipedia.org/wiki/GIMP
Редактор PDF	PDFCreator	http://www.pdfforge.org/pdfcreator
Аудиоплеер	VLC	http://www.videolan.org/vlc/

8. Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации по дисциплине

Паспорт оценочных средств по учебной дисциплине «Комплексное обеспечение информационной безопасности»

Перечень компетенций, формируемых в результате освоения учебной дисциплины

№ п/п	Код компетенции	Формулировка контролируемой компетенции	Индикаторы достижений компетенции (по дисциплине)	Темы учебной дисциплины	Этапы формирования (семестр изучения)
1	ОПК-5	Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем	ОПК-5.1. Знает современное программное и аппаратное обеспечение информационных и автоматизированных систем ОПК-5.2. Умеет разрабатывать программное и аппаратное обеспечение информационных и автоматизированных систем для решения профессиональных задач ОПК-5.3. Владеет навыками разработки программного и аппаратного обеспечения информационных и автоматизированных систем для решения профессиональных задач	Тема 1. Информационная безопасность и уровни ее обеспечения	4
				Тема 2. Стандарты информационной безопасности: "Общие критерии"	4
				Тема 3. Стандарты информационной безопасности распределенных систем	4
				Тема 4. Классификация угроз "информационной безопасности"	4
				Тема 5. Компьютерные вирусы и защита от них	4
				Тема 6. Классификация компьютерных вирусов	4
				Тема 7. Характеристика "вирусоподобных" программ	4
				Тема 8. Антивирусные программы	4
				Тема 9. Механизмы обеспечения "информационной безопасности"	4

				Тема 10. Криптография и шифрование	4
2	ОПК-6	Способен разрабатывать компоненты программно-аппаратных комплексов обработки информации и автоматизированного проектирования	ОПК-6.1. Знает аппаратные средства и платформы инфраструктуры информационных технологий, виды, назначение, архитектуру, методы разработки и администрирования программно-аппаратных комплексов объекта профессиональной деятельности ОПК-6.2. Умеет анализировать техническое задание, разрабатывать и оптимизировать программный код для решения задач обработки информации и автоматизированного проектирования ОПК-6.3. Владеет методами составления технической документации по использованию и настройке компонентов программно-аппаратного комплекса	Тема 1. Информационная безопасность и уровни ее обеспечения	4
				Тема 2. Стандарты информационной безопасности: "Общие критерии"	4
				Тема 3. Стандарты информационной безопасности распределенных систем	4
				Тема 4. Классификация угроз "информационной безопасности"	4
				Тема 5. Компьютерные вирусы и защита от них	4
				Тема 6. Классификация компьютерных вирусов	4
				Тема 7. Характеристика "вирусоподобных" программ	4
				Тема 8. Антивирус-ные программы	4
				Тема 9. Механизмы обеспечения "информационной безопасности"	4
				Тема 10. Криптография и шифрование	4
3	ПК-2	Способен осуществлять проектирование защищенных информационных систем	ПК-2.1. Знает нормативную базу, методы описания, анализа и проектирования в области обеспечения безопасности информационных систем	Тема 1. Информационная безопасность и уровни ее обеспечения	4
				Тема 2. Стандарты информационной безопасности: "Общие критерии"	4

			ПК-2.2. Умеет выбирать методы и средства проектирования защищенных информационных систем ПК-2.3. Владеет навыками разработки аппаратных и программных средств, необходимых для обеспечения безопасности информационных систем	Тема 3. Стандарты информационной безопасности распределенных систем	4
				Тема 4. Классификация угроз "информационной безопасности"	4
				Тема 5. Компьютерные вирусы и защита от них	4
				Тема 6. Классификация компьютерных вирусов	4
				Тема 7. Характеристика "вирусоподобных" программ	4
				Тема 8. Антивирусные программы	4
				Тема 9. Механизмы обеспечения "информационной безопасности"	4
				Тема 10. Криптография и шифрование	4

Показатели и критерии оценивания компетенций, описание шкал оценивания

№ п/п	Код компетенции	Индикаторы достижений компетенции	Планируемые результаты обучения по дисциплине	Контролируемые темы учебной дисциплины	Наименование оценочного средства
1	ОПК-5	ОПК-5.1. Знает современное программное и аппаратное обеспечение информационных и автоматизированных систем ОПК-5.2. Умеет разрабатывать программное и аппаратное обеспечение информационных и автоматизированных систем для решения профессиональных задач ОПК-5.3. Владеет навыками разработки программного и аппаратного обеспечения информационных и автоматизированных систем для решения профессиональных задач	**Знать:** современное программное и аппаратное обеспечение информационных и автоматизированных систем **Уметь:** разрабатывать программное и аппаратное обеспечение информационных и автоматизированных систем для решения профессиональных задач **Владеть:** навыками разработки программного и аппаратного обеспечения информационных и автоматизированных систем для решения профессиональных задач	Тема 1. Тема 2. Тема 3. Тема 4. Тема 5. Тема 6. Тема 7. Тема 8. Тема 9. Тема 10.	Вопросы для контроля усвоения теоретического материала, тестовые задания, выполнение задания на практических занятиях
2	ОПК-6	ОПК-6.1. Знает аппаратные средства и платформы инфраструктуры информационных технологий, виды, назначение, архитектуру, методы разработки и администрирования программно-аппаратных комплексов объекта профессиональной деятельности	**Знать:** аппаратные средства и платформы инфраструктуры информационных технологий, виды, назначение, архитектуру, методы разработки и администрирования программно-аппаратных комплексов объекта профессиональной деятельности	Тема 1. Тема 2. Тема 3. Тема 4. Тема 5. Тема 6. Тема 7. Тема 8. Тема 9. Тема 10.	Вопросы для контроля усвоения теоретического материала, тестовые задания, выполнение задания на практических занятиях

		ОПК-6.2. Умеет анализировать техническое задание, разрабатывать и оптимизировать программный код для решения задач обработки информации и автоматизированного проектирования ОПК-6.3. Владеет методами составления технической документации по использованию и настройке компонентов программно-аппаратного комплекса	**Уметь:** анализировать техническое задание, разрабатывать и оптимизировать программный код для решения задач обработки информации и автоматизированного проектирования **Владеть:** методами составления технической документации по использованию и настройке компонентов программно-аппаратного комплекса		
3	ПК-2	ПК-2.1. Знает нормативную базу, методы описания, анализа и проектирования в области обеспечения безопасности информационных систем ПК-2.2. Умеет выбирать методы и средства проектирования защищенных информационных систем ПК-2.3. Владеет навыками разработки аппаратных и программных средств, необходимых для обеспечения безопасности информационных систем	**Знать:** нормативную базу, методы описания, анализа и проектирования в области обеспечения безопасности **Уметь:** выбирать методы и средства проектирования защищенных информационных систем **Владеть:** навыками разработки аппаратных и программных средств, необходимых для обеспечения безопасности информационных систем	Тема 1. Тема 2. Тема 3. Тема 4. Тема 5. Тема 6. Тема 7. Тема 8. Тема 9. Тема 10.	Вопросы для контроля усвоения теоретического материала, тестовые задания, выполнение задания на практических занятиях

8.1. Тестовые задания

(низкий уровень)

1. Что удостоверяет сертификат соответствия в сфере защиты информации?

а) удостоверяет право организации заниматься деятельностью в сфере защиты информации

б) Удостоверяет соответствие помещений организации требованиям пожарной безопасности

в) удостоверяет соответствие параметров продукции требованиям технических регламентов и иных нормативно-правовых документов в сфере защиты информации

2. Какой из действующих федеральных законов является базовым в области сертификации средств защиты информации?

а) Федеральный закон «О сертификации»

б) Федеральный закон «О техническом регулировании»

в) Федеральный закон «О персональных данных»

3. Классификация и виды информационных ресурсов определены

а) Законом "Об информации, информатизации и защите информации"

б) Гражданским кодексом

в) Конституцией

4. Система защиты государственных секретов определяется Законом

а) "Об информации, информатизации и защите информации"

б) "О государственной тайне"

в) "О безопасности"

5. Конфиденциальная информация это –

а) сведения, составляющие государственную тайну

б) сведения о состоянии здоровья высших должностных лиц

в) документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ

6. Информация это –

а) сведения, поступающие от СМИ

б) только документированные сведения о лицах, предметах, фактах, событиях

в) сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления

7. По доступности информация классифицируется на

а) открытую информацию и государственную тайну

б) информацию с ограниченным доступом и общедоступную информацию

в) виды информации, указанные в остальных пунктах

8. Информация, зафиксированная на материальном носителе, с реквизитами, позволяющими ее идентифицировать, называется

а) достоверной

б) конфиденциальной

в) документированной

9. К правовым методам, обеспечивающим информационную безопасность, относятся:

а) разработка аппаратных средств обеспечения правовых данных

б) разработка и установка во всех компьютерных правовых сетях журналов учета действий

в) разработка и конкретизация правовых нормативных актов обеспечения безопасности

10. Основными источниками угроз информационной безопасности являются все указанное в списке:

а) хищение жестких дисков, подключение к сети, инсайдерство

б) перехват данных, хищение данных, изменение архитектуры системы

в) хищение данных, подкуп системных администраторов, нарушение регламента работы

11 Виды информационной безопасности:
а) персональная, корпоративная, государственная
б) клиентская, серверная, сетевая
в) локальная, глобальная, смешанная
12. Цели информационной безопасности – своевременное обнаружение, предупреждение:
а) несанкционированного доступа, воздействия в сети
б) инсайдерства в организации
в) чрезвычайных ситуаций
13. Основные объекты информационной безопасности:
а) компьютерные сети, базы данных
б) информационные системы, психологическое состояние пользователей
в) бизнес-ориентированные, коммерческие системы
14. Основными рисками информационной безопасности являются:
а) искажение, уменьшение объема, перекодировка информации
б) техническое вмешательство, выведение из строя оборудования сети
в) потеря, искажение, утечка информации
15. К основным принципам обеспечения информационной безопасности относится:
а) экономической эффективности системы безопасности
б) многоплатформенной реализации системы
в) усиления защищенности всех звеньев системы
16. Основными субъектами информационной безопасности являются:
а) руководители, менеджеры, администраторы компаний
б) органы права, государства, бизнеса
в) сетевые базы данных, фаерволлы
17. К основным функциям системы безопасности можно отнести все перечисленное:
а) установление регламента, аудит системы, выявление рисков
б) установка новых офисных приложений, смена хостинг-компании
в) внедрение аутентификации, проверки контактных данных пользователей
18. Принципом информационной безопасности является принцип недопущения:
а) неоправданных ограничений при работе в сети (системе)
б) рисков безопасности сети, системы
в) презумпции секретности
19. Принципом политики информационной безопасности является принцип:
а) невозможности миновать защитные средства сети (системы)
б) усиления основного звена сети, системы
в) полного блокирования доступа при риск-ситуациях
20. Принципом политики информационной безопасности является принцип:
а) усиления защищенности самого незащищенного звена сети (системы)
б) перехода в безопасное состояние работы сети, системы
в) полного доступа пользователей ко всем ресурсам сети, системы
21. Принципом политики информационной безопасности является принцип:
а) разделения доступа (обязанностей, привилегий) клиентам сети (системы)
б) одноуровневой защиты сети, системы
в) совместимых, однотипных программно-технических средств сети, системы
22. К основным типам средств воздействия на компьютерную сеть относится:
а) компьютерный сбой
б) логические закладки («мины»)
в) аварийное отключение питания
23. Когда получен спам по e-mail с приложенным файлом, следует:
а) прочитать приложение, если оно не содержит ничего ценного – удалить
б) сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама

в) удалить письмо с приложением, не раскрывая (не читая) его

24. Принцип Кирхгофа:

а) секретность ключа определена секретностью открытого сообщения

б) секретность информации определена скоростью передачи данных

в) секретность закрытого сообщения определяется секретностью ключа

25. Наиболее распространены угрозы информационной безопасности корпоративной системы:

а) покупка нелицензионного ПО

б) ошибки эксплуатации и неумышленного изменения режима работы системы

в) сознательного внедрения сетевых вирусов

26. Наиболее распространены угрозы информационной безопасности сети:

а) распределенный доступ клиент, отказ оборудования

б) моральный износ сети, инсайдерство

в) сбой (отказ) оборудования, нелегальное копирование данных

27. Наиболее распространены средства воздействия на сеть офиса:

а) слабый трафик, информационный обман, вирусы в интернет

б) вирусы в сети, логические мины (закладки), информационный перехват

в) компьютерные сбои, изменение администрирования, топологии

28. Утечкой информации в системе называется ситуация, характеризуемая:

а) потерей данных в системе

б) изменением формы информации

в) изменением содержания информации

29. Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:

а) целостность

б) доступность

в) актуальность

30. Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:

а) регламентированной

б) правовой

в) защищаемой

31. Разновидностями угроз безопасности (сети, системы) являются все перечисленное в списке:

а) программные, технические, организационные, технологические

б) серверные, клиентские, спутниковые, наземные

в) личные, корпоративные, социальные, национальные

32. Окончательно, ответственность за защищенность данных в компьютерной сети несет:

а) владелец сети

б) администратор сети

в) пользователь сети

Критерии и шкала оценивания по оценочному средству «Тестовые задания»

Шкала оценивания	Критерий оценивания
5 (отлично)	85 – 100% правильных ответов
4 (хорошо)	71 – 85% правильных ответов
3 (удовлетворительно)	61 – 70% правильных ответов
2 (неудовлетворительно)	60% правильных ответов и ниже

8.2. Вопросы для контроля усвоения теоретического материала
(средний уровень)

1. В чем состоят источники угроз интересам личности?
2. В чем состоят источники угроз интересам общества?
3. В чем состоят источники угроз интересам государства?
4. Перечислите виды информации и основные методы ее защиты.
5. В чем состоят национальные интересы Российской Федерации в информационной сфере и их что собой представляет их обеспечение.
6. Раскройте понятие информационно-безопасного шифрования.
7. В чем состоит сложность использования симметричных криптографических систем?
8. В чем заключаются слабости решения с помощью псевдослучайных генераторов чисел?
9. Приведите несколько примеров применения одноразовых блокнотов.
10. Расскажите о методах противодействия данной атаке.
11. Аутентификация субъектов в распределенных системах, проблемы и решения. Схема Kerberos.
12. Аудит в информационных системах. Функции и назначение аудита, его роль в обеспечении информационной безопасности.
13. Понятие электронной цифровой подписи. Процедуры формирования цифровой подписи.
14. Законодательный уровень применения цифровой подписи.
15. Методы несимметричного шифрования. Использование несимметричного шифрования для обеспечения целостности данных.
16. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
17. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.
18. Средства обеспечения информационной безопасности в ОС Windows. Разграничение доступа к данным. Групповая политика.
19. Применение файловой системы NTFS для обеспечения информационной безопасности в Windows. Списки контроля доступа к данным (ACL) их роль в разграничении доступа к данным.
20. Применение средств Windows для предотвращения угроз раскрытия конфиденциальности данных. Шифрование данных. Функции и назначение EFS.
21. Разграничение доступа к данным в ОС семейства UNIX.
22. Основные типы политики безопасности доступа к данным. Дискреционные и мандатные политики.
23. Требования к системам криптографической защиты: криптографические требования, требования надежности, требования по защите от НСД, требования к средствам разработки.
24. Законодательный уровень обеспечения информационной безопасности. Основные законодательные акты РФ в области защиты информации.
25. Функции и назначение стандартов информационной безопасности. Примеры стандартов, их роль при проектировании и разработке информационных систем.

Лектор или преподаватель, ведущий практические занятия по дисциплине производит устный опрос по пройденным теоретическим материалам и выставляет оценку в журнале с текущей успеваемостью.

Критерии и шкала оценивания по оценочному средству
«Вопросы для контроля усвоения теоретического материала»

Шкала оценивания	Критерий оценивания
5 (отлично)	Обучающийся глубоко и в полном объёме владеет программным материалом. Грамотно, исчерпывающе и логично его излагает в устной или письменной форме. При этом знает рекомендованную литературу, проявляет творческий подход в ответах на вопросы и правильно обосновывает принятые решения, хорошо владеет умениями и навыками при выполнении практических задач.
4 (хорошо)	Обучающийся знает программный материал, грамотно и по сути излагает его в устной или письменной форме, допуская незначительные неточности в утверждениях, трактовках, определениях и категориях или незначительное количество ошибок. При этом владеет необходимыми умениями и навыками при выполнении практических задач.
3 (удовлетворительно)	Обучающийся знает только основной программный материал, допускает неточности, недостаточно чёткие формулировки, непоследовательность в ответах, излагаемых в устной или письменной форме. При этом недостаточно владеет умениями и навыками при выполнении практических задач. Допускает до 30% ошибок в излагаемых ответах.
2 (неудовлетворительно)	Обучающийся не знает значительной части программного материала. При этом допускает принципиальные ошибки в доказательствах, в трактовке понятий и категорий, проявляет низкую культуру знаний, не владеет основными умениями и навыками при выполнении практических задач. Обучающийся отказывается от ответов на дополнительные вопросы.

8.3 Практическое (прикладное) задание

(высокий уровень)

Задания, выполняемые на практических занятиях:

Задание 1. Применение основ информационной безопасности для имитации действий нарушителя по раскрытию (нарушению конфиденциальности) при использовании одного и того же одноразового блокнота (гаммы) на основе побитового сложения по модулю 2 (взлом двухразового блокнота).

Задание 2. Применение основ информационной безопасности для нахождения путей противодействия угрозе раскрытия (нарушения конфиденциальности) при наличии дискреционной модели доступа.

Задание 3. Применение основ информационной безопасности для нахождения путей противодействия угрозе раскрытия (нарушения конфиденциальности) в мандатной модели доступа при наличии пары: нарушитель – высокоуровневый сообщник.

Задание 4. Изучение процессов идентификации и аутентификации в вычислительной системе посредством создания собственной программы обработки пользовательского запроса на вход в систему. Реализация атаки на процесс идентификации/аутентификации пользователя с целью определения пароля на вход в систему, а также изучение основных методов противодействия подбору пароля**.**

Задание 5. Изучение алгоритмов вызова программ, а также принципов действия атак переполнения буфера ("buffer-overflow"). Применение основ информационной безопасности для нахождения путей противодействия угрозе. Реализация на практике модели атаки переполнения буфера.

Задание 6. Изучение основных задач, моделирование и реализация на практике процесса регистрации и учета событий в ОС с целью практического применения основ защиты

информации, а также для ознакомления с системой прерываний данной операционной системы. Ознакомление с основными методами обработки результатов аудита.

Задание 7. Разработать комплекс мероприятий по защите информации от возможной утечки информации за счет постоянных электромагнитных излучений (ПЭМИ) и наводок, основанных на использовании система активной защиты (САЗ) ВОЛНА-3М указанной зоны.

Задание 8. Получение навыков по практическому применению Программно-аппаратного комплекса средств защиты информации (ПАК СЗИ) от несанкционированного доступа (НСД) «Аккорд-АМДЗ (аппаратный модуль доверенной загрузки)».

Задание 9. Применение методов и технологий испытания программного и аппаратного уровней комплексной защиты информации для проверки наличия и работоспособности встроенных программных и иных средств защиты КИС.

Задание 10. Применение методов и технологий испытания аппаратного уровня комплексной защиты информации.

Задание 11. Применение методов и технологий испытания программного и аппаратного уровней комплексной защиты информации для проведения атаки на КИС с целью установления уязвимостей.

Задание 12. Применение методов и технологий испытания программного и аппаратного уровней комплексной защиты информации для проведения атаки на КИС с целью установления уязвимостей.

Задание 13. Применение методов и технологий испытания программного и аппаратного уровней комплексной защиты информации для проведения атаки на КИС с целью установления уязвимостей.

Задание 14. Применение методов и технологий испытания программного и аппаратного уровней комплексной защиты информации для проведения атаки на КИС с целью установления уязвимостей.

Задание 15. Применение методов и технологий испытания программного и аппаратного уровней комплексной защиты информации для проведения атаки на КИС с целью установления уязвимостей.

Задание 16. Применение принципов организации, проектирования и анализа систем защиты информации и основ их комплексного построения на различных уровнях защиты.

Критерии и шкала оценивания по оценочному средству «Практическое задание»

Шкала оценивания	Характеристика знания предмета и ответов
5 (отлично)	Обучающийся полностью и правильно выполнил задание. Показал отличные знания, умения и владения навыками, применения их при решении задач в рамках усвоенного учебного материала.
4 (хорошо)	Обучающийся выполнил задание с небольшими неточностями. Показал хорошие знания, умения и владения навыками, применения их при решении задач в рамках освоенного учебного материала.
3 (удовлетворительно)	Обучающийся выполнил задание с существенными неточностями. Показал удовлетворительные знания, умения и владения навыками, применения их при решении задач.
2 (неудовлетворительно)	Обучающийся выполнил задание неправильно. При выполнении обучающийся продемонстрировал недостаточный уровень знаний, умений и владения ими при решении задач в рамках усвоенного учебного материала.

8.4 Оценочные средства для промежуточной аттестации (экзамен)

Вопросы к экзамену:

1. В чем заключается угроза распространения и утечки информации? Какие еще угрозы Вы знаете?

2. Перечислите источники угроз безопасности информационного общества.

3. Объясните понятие аудита в контексте безопасности вычислительных систем.

4. С помощью какого механизма ОС поддерживает одновременную работу нескольких программ?

5. Как реализовать перехват прерывания средствами языка Си?

6. В чем заключается задача аудита клавиатуры?

7. Как реализовать аудит клавиатуры в ОС?

8. Что необходимо для эффективного применения комплекса и поддержания соответствующего уровня защищенности ПЭВМ и информационных ресурсов?

9. В виде каких взаимодействующих между собой подсистем можно представить средства разграничения доступа к ресурсам?

10. Что такое процедура идентификации?

11. Что такое процедура аутентификации?

12. Что означает использование дискреционного принципа управления доступом?

13. Что означает использование мандатного принципа управления доступом?

14. Для чего предназначена подсистема регистрации и учета?

15. Что фиксируется в системном журнале при регистрации событий?

16. Для чего предназначена подсистема обеспечения целостности?

17. Что такое проверка на целостность?

18. Какие средства называются аппаратными?

19. Что такое несанкционированный доступ?

20. Что происходит при непосредственном несанкционированном доступе?

Критерии и шкала оценивания к промежуточной аттестации «экзамен»

Шкала оценивания	Критерий оценивания
5 (отлично)	Обучающийся глубоко и в полном объёме владеет программным материалом. Грамотно, исчерпывающе и логично его излагает в устной или письменной форме. При этом знает рекомендованную литературу, проявляет творческий подход в ответах на вопросы и правильно обосновывает принятые решения, хорошо владеет умениями и навыками при выполнении практических задач.
4 (хорошо)	Обучающийся знает программный материал, грамотно и по сути излагает его в устной или письменной форме, допуская незначительные неточности в утверждениях, трактовках, определениях и категориях или незначительное количество ошибок. При этом владеет необходимыми умениями и навыками при выполнении практических задач.
3 (удовлетворительно)	Обучающийся знает только основной программный материал, допускает неточности, недостаточно чёткие формулировки, непоследовательность в ответах, излагаемых в устной или письменной форме. При этом недостаточно владеет умениями и навыками при выполнении практических задач. Допускает до 30% ошибок в излагаемых ответах.
2 (неудовлетворительно)	Обучающийся не знает значительной части программного материала. При этом допускает принципиальные ошибки в доказательствах, в трактовке понятий и категорий, проявляет низкую культуру знаний, не владеет основными умениями и навыками при выполнении практических задач. Обучающийся отказывается от ответов на дополнительные вопросы.

9. Особенности организации обучения для лиц с ограниченными возможностями здоровья и инвалидов

При необходимости рабочая программа учебной дисциплины может быть адаптирована для обеспечения образовательного процесса инвалидов и лиц с ограниченными возможностями здоровья, в том числе с применением электронного обучения и дистанционных образовательных технологий.

Для этого требуется заявление студента (его законного представителя) и заключение психолого-медико-педагогической комиссии (ПМПК). В случае необходимости обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося), а для инвалидов также в соответствии с индивидуальной программой реабилитации инвалида могут предлагаться следующие варианты восприятия учебной информации с учетом их индивидуальных психофизических особенностей:

- создание текстовой версии любого нетекстового контента для его возможного преобразования в альтернативные формы, удобные для различных пользователей;
- создание контента, который можно представить в различных видах без потери данных или структуры, предусмотреть возможность масштабирования текста и изображений без потери качества, предусмотреть доступность управления контентом с клавиатуры;
- создание возможностей для обучающихся воспринимать одну и ту же информацию из разных источников, например, так, чтобы лица с нарушениями слуха получали информацию визуально, с нарушениями зрения – аудиально;
- применение программных средств, обеспечивающих возможность освоения навыков и умений, формируемых дисциплиной (модулем), за счёт альтернативных способов, в том числе виртуальных лабораторий и симуляционных технологий;
- применение электронного обучения, дистанционных образовательных технологий для передачи информации, организации различных форм интерактивной контактной работы обучающегося с преподавателем, в том числе вебинаров, которые могут быть использованы для проведения виртуальных лекций с возможностью взаимодействия всех участников дистанционного обучения, проведения семинаров, выступления с докладами и защиты выполненных работ, проведения тренингов, организации коллективной работы;
- применение электронного обучения, дистанционных образовательных технологий для организации форм текущего и промежуточного контроля;
- увеличение продолжительности сдачи обучающимся инвалидом или лицом с ограниченными возможностями здоровья форм промежуточной аттестации по отношению к установленной продолжительности их сдачи:
- продолжительность сдачи зачёта или экзамена, проводимого в письменной форме, – не более чем на 90 минут;
- продолжительность подготовки обучающегося к ответу на зачёте или экзамене, проводимом в устной форме, – не более чем на 20 минут;
- продолжительность выступления обучающегося при защите курсовой работы – не более чем на 15 минут.

Лист изменений и дополнений

№ п/п	Виды дополнений и изменений с указанием страниц	Дата и номер протокола заседания кафедры (кафедр), на котором были рассмотрены и одобрены изменения и дополнения	Подпись (с расшифровкой) заведующего кафедрой (заведующих кафедрами)
1.			
2.			
3.			
4.			