МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Б1.В.10
(индекс дисциплины)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Программно-аппаратные средства защиты информации
(наименование дисциплины)

по направлению подготовки
09.03.03 Прикладная информатика
направленность (профиль)
Прикладная информатика в информационной безопасности

Форма обучения: очная

Год набора: 2023

Общая трудоемкость:4 ЗЕ

Распределение часов дисциплины по семестрам

Семестр		**6**	**Итого**
Форма контроля **Вид занятий**		**зачет**	
Лекции		16	16
Лабораторные		-	-
Практические		32	32
Руководство: курсовые работы (проекты) / РГР		-	-
Промежуточная аттестация		0.25	0.25
Контактная работа		48.25	48.25
Самостоятельная работа		95.75	95.75
Контроль		-	-
Итого		**144**	**144**

Рабочую программу составил(и):

Власов Игорь Анатольевич

(должность, ученое звание, степень, Фамилия И.О.)

(должность, ученое звание, степень, Фамилия И.О.)

Рецензирование рабочей программы дисциплины:

☒ Отсутствует

☐ Рецензент

(должность, ученое звание, степень, Фамилия И.О.)

Рабочая программа дисциплины составлена на основании ФГОС ВО и учебного плана направления подготовки (специальности) 09.03.03 Прикладная информатика

Срок действия рабочей программы дисциплины до 31.08.2027

УТВЕРЖДЕНО

На заседании института инженерной и экологической безопасности

(протокол заседания № 2 от 05.09.2022).

1. Цель освоения дисциплины

Целью освоения дисциплины «Программно-аппаратные средства защиты информации» является формирование у студентов знаний о принципах построения систем защиты информации (СЗИ) в операционных системах (ОС), вычислительных сетях (ВС) и системах управления базами данных (СУБД).

Задачи дисциплины направлены на изучение:

− принципов построения систем защиты в ОС, ВС и СУБД различной архитектуры;

− средств и методов несанкционированного доступа (НСД) к ресурсам ОС, ВС и СУБД;

− принципов функционирования современных систем аутентификации;

− методик использования межсетевых экранов (МЭ);

− программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем;

− основных мер по защите информации и программных продуктов от несанкционированного доступа, модификации и изучения в автоматизированных системах.

2. Место дисциплины в структуре ОПОП ВО

Дисциплины и практики, на освоении которых базируется данная дисциплина:

- Настройка и администрирование компьютерных сетей;
- Основы управления информационной безопасностью.

Полученные знания используются при изучении следующих дисциплин:

- Техническая защита информации;
- Безопасность компьютерных сетей;
- Безопасность баз данных.

3. Планируемые результаты обучения

Формируемые и контролируемые компетенции (код и наименование)	**Индикаторы достижения компетенций** (код и наименование)	**Планируемые результаты обучения**
ПК-3 Способен оценивать угрозы безопасности информации операционных систем и сетей	ПК-3.4 Использует принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации	Знать: - основные принципы построения подсистем защиты компьютерной информации в операционных системах и в пользовательских программных приложениях; - принципы функционирования и обеспечения защиты программно-аппаратных средств информационной безопасности;
		Уметь: - оценивать эффективность и надежность защиты ОС, ВС и СУБД; - выявлять слабости защиты ОС, ВС и СУБД и использовать их для вскрытия защиты;
		Владеть: - эффективного использования

Формируемые и контролируемые компетенции (код и наименование)	**Индикаторы достижения компетенций** (код и наименование)	**Планируемые результаты обучения**
		программно-аппаратные средства обеспечения информационной безопасности;
	ПК-3.5 Применяет меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты.	Знать: - проблемы и направления развития аппаратных и программных средств защиты информации;
		Уметь: - применять и администрировать средства программно-аппаратной защиты информации
		Владеть: - методами защиты информации в операционных системах и в пользовательских приложениях;
	ПК-3.6 Демонстрирует владение навыками эффективного использования программно-аппаратные средства обеспечения информационной безопасности	Знать: - сертифицированные и перспективные программно-аппаратные средства, и методы защиты компьютерной информации
		Уметь: - планировать программно-аппаратную подсистему безопасности организации;
		Владеть: - навыками использования межсетевых экранов и систем обнаружения вторжений и других СЗИ

4. Структура и содержание дисциплины

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
Модуль 1	Лек	Тема 1 Предмет и задачи программно-аппаратной защиты информации Место программно-аппаратных методов и средств в комплексных системах защиты информации. Основные термины и определения. Структура и состав систем защиты информации и комплексов средств защиты. Определение места программно-аппаратных средств защиты информации в общей проблеме информационной безопасности. Нормативно-правовые и технические требования к программно-аппаратным средствам защиты информации.	5	2		-	
Модуль 1	Ср	Тема 1 Предмет и задачи программно-аппаратной защиты информации	5	12			
Модуль 1	Лек	Тема 2 Проектирование и реализация комплексов средств защиты информации. Проблемы проектирования и реализации механизмов защиты Техническое проектирование и реализация комплексов средств защиты. Жизненный цикл корпоративный системы. Обзор подходов к созданию комплексов средств защиты. Проблемы проектирования и реализации защищенных АС. Основные принципы создания программно-аппаратных средств обеспечения информационной безопасности. Программно-аппаратные средства, реализующие отдельные функциональные требования по	5	2		-	

		защите. Их принципы действия и технологические особенности					
Модуль 1	Пр	Тема 2 Проектирование и реализация комплексов средств защиты информации. Проблемы проектирования и реализации механизмов защиты Методика проектирования СЗИ. Построение модели для выбранного объекта	5	4			Отчет по практическому занятию №1
Модуль 1	Ср	Тема 2 Проектирование и реализация комплексов средств защиты информации. Проблемы проектирования и реализации механизмов защиты	5	12			
Модуль 1	Лек	Тема 3 Теоретические основы реализации механизмов защиты информации Задачи и методологические основы использования аппаратных средств защиты информации в компьютерах. Технические требования стандартов к программно-аппаратным средствам защиты информации. Формальные модели и политики управления доступом. Подсистема обеспечения целостности. Контроль целостности. Антивирусная защиты. Резервное копирование. Подсистема регистрации и учёта событий. Криптографическая подсистема.	5	2			
Модуль 1	Ср	Тема 3 Теоретические основы реализации механизмов защиты информации	5	12			
Модуль 1	Лек	Тема 4 Механизмы защиты, реализуемые на базе программных продуктов фирмы Microsoft Подсистема разграничения доступа. Подсистема регистрации и учёта. Подсистема обеспечения целостности. Криптографическая подсистема. Интерфейс администратора безопасности. Понятие домена. Особенности установления доверительных отношений. Создание и	5	2		-	

		удаление бюджетов пользователей.					
Модуль 1	Пр	Тема 4 Механизмы защиты, реализуемые на базе программных продуктов фирмы Microsoft Обеспечение безопасности доступа к данным информационной системы организации с помощью продуктов Microsoft и Aladdin. Типовые решения.	5	4			Отчет по практическому занятию №2
Модуль 1	Ср	Тема 4 Механизмы защиты, реализуемые на базе программных продуктов фирмы Microsoft	5	12			
Модуль 1	Лек	Тема 5 Механизмы защиты, реализуемые на базе ОС семейства Linux Основные компоненты подсистемы защиты LINUX. Файловая система – как основа подсистемы защиты. Права доступа к элементам файловой системы. Управление процессами. Создание и удаление бюджетов пользователей. Основные проблемы с безопасностью и возможные решения в UNIX-подобных системах. Подсистемы. Пересборка ядра ОС. Вывод системы из нестабильного состояния: поиски и устранение неполадок.	5	2		-	
Модуль 1	Пр	Тема 5 Механизмы защиты, реализуемые на базе ОС семейства Linux Настройка встроеннвх систем безопасности Linux	5	4			Отчет по практическому занятию №3
Модуль 1	Ср	Тема 5 Механизмы защиты, реализуемые на базе ОС семейства Linux	5	12			
Модуль 1	Лек	Тема 6 Средства защиты информации, реализованные в активном сетевом оборудовании Используемое сетевое оборудование. Его классификация. Средства обеспечения безопасности корпоративных сетей. Основные защитные механизмы и примеры их реализации. Особенности	5	2			

		существующих свободно-распространяемых программных реализаций межсетевых экранов. Фильтрация пакетов. Межсетевые экраны уровня соединения. Межсетевые экраны прикладного уровня. Межсетевые экраны с динамической фильтрацией пакетов. Межсетевые экраны инспекции состояния. Межсетевые экраны уровня ядра. Требования к показателям защищенности межсетевых экранов. МЭ на платформе Windows. МЭ IPTables на платформе Linux. Установка и настройка Web Application Firewal					
Модуль 1	Пр	Тема 6 Средства защиты информации, реализованные в активном сетевом оборудовании Разработка МЭ на платформе Windows. Настройка брэндмауэра.	5	4			Отчет по практическому занятию №4
Модуль 1	Пр	Тема 6 Средства защиты информации, реализованные в активном сетевом оборудовании Разработка МЭ IPTables на платформе Linux	5	4			Отчет по практическому занятию №5
Модуль 1	Пр	Тема 6 Средства защиты информации, реализованные в активном сетевом оборудовании Установка и настройка Web Application Firewal	5	4			Отчет по практическому занятию №6
Модуль 1	Ср	Тема 6 Средства защиты информации, реализованные в активном сетевом оборудовании	5	12			
Модуль 1	Лек	Тема 7. Средства защиты информации, реализованные в прикладном программном обеспечении Возможности реализации средств защиты на прикладном уровне. Использование API и библиотек. Использование системных вызовов. Реализация собственных библиотек. Примеры реализации механизмов защиты на прикладном уровне.	5	2			

		Стандарты разработки ПО. Разработка безопасного программного кода, ГОСТ Р 56939-2016 «Разработка безопасного программного обеспечения».					
Модуль 1	Ср	Тема 7. Средства защиты информации, реализованные в прикладном программном обеспечении	5	12			
Модуль 1	Лек	Тема 8 Программно-аппаратные средства защиты информации от несанкционированного доступа Применение программно-аппаратных комплексов SecretNet , Соболь, Континент, Dallas Lock. Установка и регистрация в системе защиты. Создание учетных записей. Реализация дискреционной и мандатной моделей разграничения до тупа. Обеспечение замкнутости программной среды. Контроль целостности. Регистрация событий. Гарантированное удаление данных.	5	2			
Модуль 1	Пр	Тема 8 Программно-аппаратные средства защиты информации от несанкционированного доступа Изучение методов защиты локальной ПЭВМ от НСД к информации, от несанкционированного копирования информации, идентификации и аутентификации субъектов в АС при помощи программно-аппаратного комплекса Secret Net 5.0 и электронного ключа "Соболь". Установка и настройка ПАК Континент	5	4			Отчет по практическому занятию №7
Модуль 1	Пр	Тема 8 Программно-аппаратные средства защиты информации от несанкционированного доступа Изучение методов защиты локальной ПЭВМ от НСД к информации, от несанкционированного копирования информации, идентификации и аутентификации субъектов в АС при помощи программно-аппаратного комплекса Dallas Lock. Настройка ПАК.	5	4			Отчет по практическому занятию №8

Модуль 1	Ср	Тема 8 Программно-аппаратные средства защиты информации от несанкционированного доступа		11.75			
	ПА	Сдача зачета (итоговый тест/сдача зачета устно (письменно)	5	0,25		-	Банк тестовых заданий /Вопросы к зачету
			Итого:	**144**			

5. Образовательные технологии

Технология	Формы обучения	Методы обучения
Технология традиционного обучения – организация учебного процесса в вузе, основанная на лекционно-семинарско-зачетной формах обучения	Лекция. Практическое занятие. Самостоятельная работа. Индивидуальное домашнее задание.	Наглядные, словесные, практические.
Технология модульного обучения – организация учебного процесса для полного овладения содержанием образовательных программ на основе независимых учебных модулей с учетом индивидуальных интересов и возможностей субъектов образовательного процесса.	Лекция-консультация. Семинар с использованием метода анализа конкретных ситуаций.	Решение ситуационных задач. Презентационный метод. Самостоятельная работа. Консультация. Индивидуальная работа.
Информационные технологии – специальные способы, программные и технические средства (кино, аудио – и видеосредства, компьютеры) для работы с информацией	Лекция-пресс-конференция. Визуальная лекция.	Презентационный метод.
	Формы и методы обучения	
Дистанционное обучение	**Сетевая технология** – изучение курса (учебной дисциплины) посредством электронных учебно-методических материалов, размещенных в обучающей среде с использованием компьютера, подключенного к сети Интернет. **CD-технология** – изучение курса (учебной дисциплины), представленного студенту в виде автономной электронной обучающей системы и электронной версии учебно-методических материалов на CD-диске.	

6. Методические указания по освоению дисциплины

6.1. Рекомендации по освоению лекционного материала, подготовке к лекциям

Лекции являются одним из основных видов учебных занятий в высшем учебном заведении. В ходе лекционного курса проводится изложение современных научных материалов в систематизированном виде, а также разъяснение наиболее трудных вопросов учебной дисциплины. При изучении дисциплины следует помнить, что лекционные занятия являются направляющими в большом объеме научного материала. Большую часть знаний студент должен набирать самостоятельно из учебников и научной литературы. Конспекты лекций рекомендуется использовать при подготовке к лабораторным занятиям, экзамену, контрольным тестам, при выполнении самостоятельных заданий.

. 6.2. Рекомендации по организации самостоятельной работы

Самостоятельная работа включает изучение литературы, поиск информации в сети Интернет, подготовку к тестам, экзамену. Необходимо разобраться в основных понятиях. Записать возникшие вопросы и найти ответы на них на занятиях, либо

разобрать их с преподавателем. Подготовку к экзамену необходимо начинать заранее. Следует проанализировать научный и методический материал учебников, учебно-методических пособий, конспекты лекций. Знать формулировки терминов и уметь их четко воспроизводить.

7. Оценочные средства

7.1. Паспорт оценочных средств

Семестр	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
6	ПК-3	Протоколы практических заданий №1-8
		Вопросы к зачету №№1-45 Темы рефератов Банк тестовых заданий 1-350

7.2. Типовые задания или иные материалы, необходимые для текущего контроля

7.2.1 Реферат Виды аппаратных средств защиты информации

7.2.2 Реферат Программные средства защиты информации

7.2.3. Выполнение практических заданий

Темы Практических заданий

№	Тема
1	Методика проектирования СЗИ. Построение модели для выбранного объекта
2	Обеспечение безопасности доступа к данным информационной системы организации с помощью продуктов Microsoft и Aladdin. Типовые решения.
3	Настройка встроеннвх систем безопасности Linux
4	Разработка МЭ на платформе Windows.Настройка брэндмауэра.
5	Разработка МЭ IPTables на платформе Linux
6	Установка и настройка Web Application Firewal
7	Изучение методов защиты локальной ПЭВМ от НСД к информации, от несанкционированного копирования информации, идентификации и аутентификации субъектов в АС при помощи программно-аппаратного комплекса Secret Net 5.0 и электронного ключа "Соболь". Установка и настройка ПАК.
8	Изучение методов защиты локальной ПЭВМ от НСД к информации, от несанкционированного копирования информации, идентификации и аутентификации субъектов в АС при помощи программно-аппаратного комплекса Dallas Lock. Настройка ПАК.

Типовой(ые) пример(ы) задания(ий)

При выполнении практических заданий студенты отрабатывают методику проектирования СЗИ, настраивают системы безопасности Linux, устанавливают и настраивают Web Application Firewal, ПАК Соболь и другие СЗИ.

Краткое описание и регламент выполнения

1. Изучить теоретический материал и нормативно-правовую базу.
2. Оформить отчет о практической работе в соответствии с требованиями к оформлению практических работ в соответствии с тематикой задания.

Критерии оценки:

- оценка «зачтено» выставляется студенту, если практическое задание выполнено грамотно или имеет несущественные замечания, выполнен отчет по работе.
- оценка «не зачтено» выставляется студенту, если практическое задание не выполнено, имеет грубые ошибки, не подготовлен отчет.

7.2.2.
Типовой пример тестового задания

Классификация систем обнаружения вторжений

Выберите один или несколько вариантов ответа:

1) по способам реагирования
2) по решаемым задачам
3) по способу сбора информации
4) по методам анализа

Критерии оценки:

Минимальное количество баллов 1. Баллы начисляются автоматически пропорционально правильным ответам.

7.3. Оценочные средства для промежуточной аттестации по итогам освоения дисциплины

7.3.1. Вопросы к промежуточной аттестации

Семестр 6

№ п/п	Вопросы к зачету
1.	Нормативно-правовые и технические требования к программно-аппаратным средствам защиты информации
2.	Понятие несанкционированного доступа (НСД) к информации
3.	Настройка политики безопасности операционной системы
4.	В чем заключается модель дискреционной политики безопасности ?
5.	Групповая политика в доменах Windows
6.	Методы и средства защиты информации от НСД в локальных ПЭВМ

7.	Типы контроля безопасности: потоковый, контроль вывода, контроль доступа
8.	Технологии доверенной загрузки операционной системы
9.	Принципы сертификации средств защиты информации
10.	Управление средствами аутентификации в Linux и Windows
11.	Применение типовых моделей управления доступом в операционных системах
12.	Как соотносятся матрица доступа и ролевой доступ?
13.	Средства обеспечения защиты информации в СУБД
14.	Средства и методы обеспечения целостности данных СУБД
15.	Методы внедрения программных закладок
16.	Реализация защиты от вредоносного программного кода
17.	Механизм сетевых атак на браузеры
18.	Управление процессами. Создание и удаление бюджетов пользователей
19.	Организация и администрирование работы различных типов межсетевых экранов.
20.	Межсетевые экраны, их типы и конфигурация
21.	Организация и администрирование работы различных типов межсетевых экранов.
22.	Состав и возможности ПО СЗИ SecretNet
23.	Состав и возможности ПО СЗИ Dallas Lock
24.	Состав и возможности ПО СЗИ Континент
25.	Протоколы аутентификации и идентификации пользователей в компьютерных сетях. RDP, RDG, VPN, VDI
26.	Организация и методики контроля облачных сервисов
27.	Классификация систем обнаружения вторжений
28.	Методы обхода сетевых систем обнаружения вторжений
29.	Понятие о сигнатуре вредоносного программного кода
30.	Деструктивные функции вредоносных программ
31.	Механизмы вирусного заражения
32.	Методы работы с пользователями по профилактике заражения вирасами
33.	Понятие о «троянских» программах и их функциях. Программы-«джойнеры
34.	Механизмы статического скрытия вредоносного программного кода
35.	Сетевые вирусы: жизненный цикл, особенности функционирования, особенности противодействия сетевым вирусам
36.	Основные меры по защите от вирусов - шифровальщиков
37.	Что такое программный вирус и какова его природа?
38.	Какие программные модули входят в состав программного комплекса ViPNet?
39.	Для чего служит ключевой набор (ViPNet)?
40.	Порядок сертификации новой ЭП абонента (ViPNet)?

41.	Администрирование канала на VipNet
42.	ПАК VipNet Coordinator, возможности, назначение, администрирование
43.	Электронная подпись, принцип работы, сертификаты, УЦ
44.	Принцип действия, достоинства и недостатки аппаратных устройств на основе электронных (магнитных) идентификаторов
45.	Биометрическая идентификация

7.3.2. Критерии и нормы оценки

Семестр	**Форма проведения промежуточной аттестации**	**Критерии и нормы оценки**	
6	Зачет (письменно/по накопительному рейтингу)	«зачтено»	55-100 баллов
		«не зачтено»	0-54 баллов

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Обязательная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно-методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
1	Казарин О. В., Забабурин А. С.	Программно-аппаратные средства защиты информации	учебное пособие	2022	
2	Галатенко В.А.	Идентификация и аутентификация, управление доступом	Эл.ресурс	2021	http://citforum.ru/security/articles/galatenko/- (дата обращения - 17.10.2021)
3	Прохорова О. В.	Информационная безопасность и защита информации	учебное пособие	2022	

8.2. Дополнительная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно-методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
1	Шаньгин В.Ф.	Защита компьютерной информации. Эффективные методы и средства	учебное пособие	2019	https://e.lanbook.com/book/1122

8.3. Перечень профессиональных баз данных и информационных справочных систем

Интернет-портал для ИТ-специалистов - http://www.habrahabr.ru/
Интернет-портал ресурсов по информационной безопасности - http//www.all-ib.ru
Консультант Плюс - http://www.consultant.ru/
Официальный портал правовой информации - http://pravo.gov.ru/
Официальный сайт Федеральной службы по техническому и экспортному контролю - http://www.fstec.ru/

8.4. Перечень программного обеспечения

№ п/п	Наименование ПО	Реквизиты договора (дата, номер, срок действия)
1	Windows	Windows (Договор № 690 от 19.05.2015г., срок действия - бессрочно);
2	OfficeStandart	OfficeStandart (Договор № 690 от 19.05.2015г., срок действия - бессрочно; Договор № 727 от 20.07.2016г., срок действия - бессрочно)
3.	Консультант+	Консультант+ (Договор №1522 от 25.12.2015, срок действия - бессрочно)

8.5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)	Перечень основного оборудования
1	Аудитория веб-конференций. Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации Э-705	Стол преподавательский, экран телевизионный, роутер, стойка для телевизора, веб. камера, транспарант-перетяжка, ширма, наушники, компьютер с выходом в Интернет.
2	"Аудитория веб-конференций. Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации.	Столы ученические., стол преподавательский, стулья, доска (маркерная), кафедра напольная, ПК , телевизор.

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)	Перечень основного оборудования
	УЛК -310	
3	Помещение для самостоятельной работы обучающихся Г-401	Столы, стулья, компьютеры
4	Помещение для самостоятельной работы обучающихся Д -409	Столы-парты двухместные, стулья, стол преподавательский-, стул преподавательский, передвижная доска, экран, процессор, проектор, компьютерные столы, компьютеры для студентов с выходом в сеть интернет, компьютер преподавателя, сетевой шкаф