Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Выборнова Любовь Алексеевна
Должность: Ректор
Дата подписания: 30.10.2026 13:35:47
Уникальный программный ключ:
c3b3b9c625f6c113afa2a2c42baff9e05a38b76e

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Поволжский государственный университет сервиса» (ФГБОУ ВО «ПВГУС»)

Высшая школа интеллектуальных систем и кибертехнологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б.1.В.03.06 «Средства защиты программного обеспечения»

Направление подготовки:

10.03.01 «Информационная безопасность»

Направленность (профиль):

«Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)»

Квалификация выпускника: **бакалавр**

Тольятти 2025

Рабочая программа дисциплины «Средства защиты программного обеспечения» разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования – бакалавриат по направлению подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Министерства науки и высшего образования Российской Федерации от 17.11.2020 г. № 1427.

Составители:

старший преподаватель	Ю.С. Мунирова
(ученая степень, ученое звание)	(ФИО)

РПД обсуждена на заседании ученого совета Высшей школы интеллектуальных систем и кибертехнологий

«23» _05_ 2025_ г., протокол № _10_

Директор	к.э.н., доцент	О.А. Филиппова
	(уч.степень, уч.звание)	(ФИО)

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1.1. Цель освоения дисциплины

Целями освоения дисциплины являются:

– формирование у обучающихся системных теоретических знаний об основных характеристиках, достоинствах и недостатках современных средств защиты программного обеспечения;

– формирование умения применять средства криптографической и технической защиты программного обеспечения для решения задач профессиональной деятельности;

– формирование навыков выполнения работ по установке, настройке и обслуживанию средств защиты программного обеспечения.

-формирование у обучающихся общепрофессиональных компетенций *в области использования информационно-коммуникационных технологий и т.п.*

-формирование у обучающихся профессиональных компетенций, необходимых для решения задач профессиональной деятельности

1.2. Перечень планируемых результатов обучения по дисциплине

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Планируемые результаты обучения по дисциплине**	**Основание (ПС)** *для профессиональных компетенций
ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ИОПК-9.1. Знает основные характеристики, достоинства и недостатки средств криптографической и технической защиты информации в автоматизированных системах ИОПК-9.2. Применяет средства криптографической и технической защиты информации от «утечки» ИОПК-9.3. Применяет технические средства контроля эффективности применяемых мер защиты информации	Знает: – основные характеристики, достоинства и недостатки современных средств защиты программного обеспечения; методы контроля эффективности применяемых средств защиты Умеет: – применять средства криптографической и технической защиты программного обеспечения; оценивать эффективность применяемых средств защиты Владеет: – навыками применения технических средств контроля эффективности мер защиты программного обеспечения	
ПК-1. Способен выполнять работы по установке, настройке и	ИПК-1.1. Устанавливает, настраивает и обслуживает	Знает: – порядок установки, настройки и обслуживания средств защиты программного	06.032 «Специалист по безопасности компьютерных систем и сетей»

обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	программное обеспечение, программно-аппаратные и технические средства защиты информации с соблюдением требований по защите информации	обеспечения в соответствии с технической документацией и требованиями по защите информации Умеет: – устанавливать и настраивать программные, программно-аппаратные и технические средства защиты программного обеспечения Владеет: – навыками обслуживания средств защиты программного обеспечения в процессе эксплуатации	

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина относится к части, формируемой участниками образовательных отношений, Блока 1. Дисциплины (модули) программы бакалавриата (Б1.В.03 Профессиональный модуль).

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1. Объем и структура дисциплины

Общая трудоёмкость дисциплины составляет **4 з.е. (144 час.)**, их распределение по видам работ представлено в таблице.

Виды учебных занятий и работы обучающихся	Трудоемкость, час
Общая трудоемкость дисциплины, час	**144**
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего), в т.ч.:	**106/66**
занятия лекционного типа (лекции)	32/24
занятия семинарского типа (семинары, практические занятия, практикумы, коллоквиумы и иные аналогичные занятия)	56/32
лабораторные работы	18/10
Самостоятельная работа, всего	**11/69**
Контроль (часы на экзамен)	**27/9**
Промежуточная аттестация	**Экзамен**

Примечание: *-/- объем часов соответственно для очной, очно-заочной форм обучения*

Дисциплина реализуется посредством проведения контактной работы с обучающимися (включая проведение текущего контроля успеваемости), самостоятельной работы обучающихся и промежуточной аттестации.

В процессе освоения дисциплины может применяться электронное обучение и дистанционные образовательные технологии.

В процессе освоения дисциплины обучающиеся обеспечены доступом к электронной информационно-образовательной среде и электронно-библиотечным системам.

3.2. Содержание дисциплины, структурированное по темам

Планируемые результаты освоения: код формируемой компетенции и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы				Формы текущего контроля (наименование оценочного средства)
		Контактная работа			Самостоятельная работа, час	
		Лекции, час	Лабораторные работы, час	Практические занятия, час		
ОПК-9 ИОПК-9.1	**ТЕМА 1. КЛАССИФИКАЦИЯ СРЕДСТВ ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ** Основное содержание: 1. Понятие и назначение средств защиты программного обеспечения. 2. Классификация средств защиты программного обеспечения по функциональному назначению. 3. Общая характеристика достоинств и недостатков различных классов средств защиты.	4/4				Устный опрос
	Практическое занятие № 1. Сравнительный анализ классов средств защиты программного обеспечения			7/4		
	Лабораторная работа № 1 Классификация средств защиты программного обеспечения по функциональному назначению		2/4			
	Самостоятельная работа				1/4	Самостоятельное изучение методических материалов

ОПК-9 ИОПК-9.1	**ТЕМА 2. СРЕДСТВА ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА** Основное содержание: 1. Назначение и принципы работы средств защиты информации от несанкционированного доступа (СЗИ от НСД). 2. Функциональные возможности СЗИ от НСД: разграничение доступа, идентификация, аутентификация.	4/4				Практическое задание
	Практическое занятие № 2. Установка и настройка средства защиты информации от несанкционированного доступа			7/4		
	Лабораторная работа № 2 Функциональные возможности СЗИ от НСД: разграничение доступа, идентификация, аутентификация.		2/4			
	Самостоятельная работа				1/4	
ОПК-9 ИОПК-9.2	**ТЕМА 3. КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ** Основное содержание: 1. Назначение и характеристики криптографических средств защиты программного обеспечения. 2. Средства электронной подписи программного обеспечения. 3. Отечественные сертифицированные криптографические средства защиты информации.	4/4				Доклад/сообщение
	Практическое занятие № 3. Применение криптографического средства защиты информации для контроля целостности ПО			7/4		
	Лабораторная работа № 2 Отечественные сертифицированные		2/4			

	криптографические средства защиты информации					
	Самостоятельная работа				1/4	Самостоятельное изучение методических материалов
ОПК-9 ИОПК-9.3	**ТЕМА 4. КОНТРОЛЬ ЦЕЛОСТНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ** Основное содержание: 1. Средства контроля целостности программного обеспечения. 2. Методы обнаружения несанкционированных изменений программного кода. 3. Технические средства контроля эффективности применяемых мер защиты.	4/4				Практическое задание
	Практическое занятие № 4. Настройка средства контроля целостности программного обеспечения			7/4		
	Лабораторная работа № 4 . Технические средства контроля эффективности применяемых мер защиты		2/4			
	Самостоятельная работа				1/4	Самостоятельное изучение методических материалов
ПК-1 ИПК-1.1	**ТЕМА 5. АНТИВИРУСНЫЕ СРЕДСТВА ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ** Основное содержание: 1. Принципы работы антивирусных средств защиты. 2. Классификация антивирусных средств: сигнатурный, эвристический, поведенческий анализ. 3. Установка, настройка и обновление антивирусного программного обеспечения.	4/4				Устный опрос / тестирование
	Практическое занятие № 5. Установка, настройка и обновление антивирусного			7/4		

	средства защиты					
	Лабораторная работа № 5 Классификация антивирусных средств: сигнатурный, эвристический, поведенческий анализ.		2/4			
	Самостоятельная работа				1/4	Самостоятельное изучение методических материалов
ПК-1 ИПК-1.1	**ТЕМА 6. СРЕДСТВА ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ** Основное содержание: 1. Назначение и принципы работы систем обнаружения вторжений (IDS) и предотвращения вторжений (IPS). 2. Настройка правил и сигнатур систем обнаружения вторжений. 3. Средства класса EDR и sandboxing для защиты программного обеспечения.	4/4				Практическое задание
	Практическое занятие № 6. Настройка системы обнаружения вторжений для защиты программного обеспечения			7/4		
	Лабораторная работа № 6 . Настройка правил и сигнатур систем обнаружения вторжений		2/4			
	Самостоятельная работа				2/4	Самостоятельное изучение методических материалов

ПК-1 ИПК-1.1	**ТЕМА 7. ОБСЛУЖИВАНИЕ СРЕДСТВ ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ** Основное содержание: 1. Порядок обслуживания и сопровождения средств защиты программного обеспечения. 2. Обновление баз сигнатур и правил средств защиты. 3. Контроль работоспособности установленных средств защиты.	4/4				Практическое задание / тестирование
	Практическое занятие № 7. Обслуживание и контроль работоспособности средств защиты программного обеспечения			7/4		
	Лабораторная работа №7 Контроль работоспособности установленных средств защиты		2/4			
	Самостоятельная работа				2/4	Самостоятельное изучение методических материалов
ОПК-9, ИОПК-9.3; ПК-1 ИПК-1.1	**ТЕМА 8. ОЦЕНКА ЭФФЕКТИВНОСТИ СРЕДСТВ ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ** Основное содержание: 1. Показатели и критерии оценки эффективности средств защиты программного обеспечения. 2. Методика контроля эффективности применяемых мер защиты. 3. Составление отчета по результатам оценки эффективности средств защиты.	4/4				Практическое задание
	Практическое занятие № 8. Оценка эффективности установленных средств защиты программного обеспечения			7/4		
	Лабораторная работа №8 Показатели и критерии оценки эффективности средств защиты программного обеспечения		2/4			
	Самостоятельная работа				2/4	Самостоятельное изучение

						методических материалов
	ИТОГО	**32/24**	**18/10**	**56/32**	**11/69**	

Примечание: *-/- объем часов соответственно для очной, очно-заочной форм обучения*

4. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

4.1. Общие методические рекомендации по освоению дисциплины, образовательные технологии

Дисциплина реализуется посредством проведения контактной работы с обучающимися (включая проведение текущего контроля успеваемости), самостоятельной работы обучающихся и промежуточной аттестации.

При проведении учебных занятий по дисциплине обеспечивается развитие у обучающихся навыков системного и критического мышления, практических умений и владений, необходимых для решения профессиональных задач в области информационной безопасности (включая проведение интерактивных лекций, лабораторных и практических занятий, разбора практических ситуаций).

Преподавание дисциплины ведется с применением следующих видов образовательных технологий:

- балльно-рейтинговая технология оценивания;
- электронное обучение;
- проблемное обучение;
- разбор конкретных ситуаций (кейс-метод);
- информационные технологии, применяемые в электронной информационно-образовательной среде университета.

Для оценки знаний, умений, навыков и уровня сформированности компетенций по дисциплине применяется балльно-рейтинговая система контроля и оценки успеваемости студентов. Максимальное количество баллов в семестре – 100.

4.2. Методические указания для обучающихся по освоению дисциплины на занятиях лекционного типа

Лекционный курс предполагает систематизированное изложение основных вопросов тематического плана. В ходе лекционных занятий раскрываются базовые вопросы в рамках каждой темы дисциплины, обозначаются ключевые аспекты тем, а также делаются акценты на наиболее сложные и важные положения изучаемого материала.

Лекционные занятия проводятся в аудитории с применением мультимедийного проектора в виде учебной презентации или в ЭИОС университета.

Отдельные вопросы предлагаются для самостоятельного изучения (конспектируются).

Материалы лекций являются опорной основой для подготовки обучающихся к практическим (лабораторным) занятиям, выполнения заданий самостоятельной работы, а также к мероприятиям текущего контроля успеваемости и промежуточной аттестации по дисциплине.

4.3. Методические указания для обучающихся по освоению дисциплины на занятиях семинарского и лабораторного типа

Практические (лабораторные) занятия представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы дисциплины. Основной формой проведения занятий является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также решение практических задач и выполнение заданий на персональном компьютере.

Практические (лабораторные) занятия обучающихся обеспечивают:

- проверку и уточнение знаний, полученных на лекциях;
- получение умений и практических навыков по учебному материалу дисциплины;
- подведение итогов занятий по рейтинговой системе, согласно технологической карте дисциплины.

Занятия организуются, в том числе, в форме практической подготовки, которая предусматривает участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.

Практическая подготовка предусматривает: выполнение всех заданий на практических занятиях

4.4. Методические указания по самостоятельной работе обучающихся

Самостоятельная работа обеспечивает подготовку обучающегося к аудиторным занятиям и мероприятиям текущего контроля и промежуточной аттестации по изучаемой дисциплине.

Самостоятельная работа студентов включает:

- изучение учебной литературы и нормативных документов по курсу;
- подготовку к практическим (лабораторным) занятиям;
- решение практических ситуаций и задач;
- работу с ресурсами информационно-телекоммуникационной сети «Интернет»;
- подготовку к тестированию по темам курса;
- подготовку к промежуточной аттестации по курсу.

Для обеспечения самостоятельной работы обучающихся используется электронный учебный курс, созданный в ЭИОС университета http://sdo.tolgas.ru/.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Вся литература, включенная в данный перечень, представлена в виде электронных ресурсов в электронной библиотеке университета (ЭБС). Литература, используемая в печатном виде, представлена в научной библиотеке университета в объеме не менее 0,25 экземпляров на одного обучающегося.

Основная литература:

1. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В. Ф. Шаньгин. – Москва : ИД «ФОРУМ». – Текст : электронный.

2. Мельников, В. П. Информационная безопасность и защита информации : учебное пособие / В. П. Мельников, С. А. Клейменов, А. М. Петраков. – Москва : Академия. – Текст : электронный.

3. Казарин, О. В. Безопасность программного обеспечения компьютерных систем : монография / О. В. Казарин. – Москва : МГУЛ. – Текст : электронный.

Дополнительная литература:

4. Грушо, А. А. Теоретические основы компьютерной безопасности : учебное пособие / А. А. Грушо, Э. А. Применко, Е. Е. Тимонина. – Москва : Академия. – Текст : непосредственный.

5. Бирюков, А. А. Информационная безопасность: защита и нападение : учебное пособие / А. А. Бирюков. – Москва : ДМК Пресс. – Текст : электронный.

5.2. Профессиональные базы данных, информационно-справочные системы, интернет-ресурсы

1. Реестр сертифицированных средств защиты информации ФСТЭК России : сайт. – URL: https://fstec.ru – Текст : электронный.

2. Реестр российского программного обеспечения : сайт. – URL: https://reestr.digital.gov.ru – Текст : электронный.

3. Банк данных угроз безопасности информации ФСТЭК России (БДУ) : сайт. – URL: https://bdu.fstec.ru – Текст : электронный.

4. eLIBRARY.RU : научная электронная библиотека : сайт. – URL: https://elibrary.ru – Текст : электронный.

5. Электронная библиотечная система Поволжского государственного университета сервиса : сайт / ФГБОУ ВО «ПВГУС». – Тольятти. – URL: http://elib.tolgas.ru – Режим доступа: для авториз. пользователей. – Текст : электронный.

5.3. Программное обеспечение

Информационное обеспечение учебного процесса по дисциплине осуществляется с использованием следующего программного обеспечения (лицензионного и свободно распространяемого), в том числе отечественного производства:

№ п/п	Наименование	Условия доступа
1	Средство защиты информации от несанкционированного доступа (сертифицированное)	из компьютерных классов университета (лицензионный договор)
2	Антивирусное программное обеспечение отечественного производства	из внутренней сети университета (лицензионный договор)
3	Система обнаружения вторжений (демонстрационная	из компьютерных классов университета (лицензионный /

	версия)	свободно распространяемый программный продукт)
4	КонсультантПлюс	из внутренней сети университета (лицензионный договор)
5	СДО MOODLE	из любой точки, в которой имеется доступ к сети Интернет (лицензионный договор)

6. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных учебным планом и рабочей программой дисциплины, оснащенные оборудованием и техническими средствами обучения.

Занятия лекционного типа. Учебные аудитории для занятий лекционного типа укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации (стационарные или переносные наборы демонстрационного оборудования – проектор, экран, компьютер/ноутбук), учебно-наглядные пособия (презентации по темам лекций), обеспечивающие тематические иллюстрации, соответствующие данной программе дисциплины.

Занятия семинарского и лабораторного типа. Учебные аудитории (компьютерные классы) для занятий семинарского и лабораторного типа укомплектованы мебелью, компьютерной техникой с необходимым программным обеспечением и техническими средствами обучения.

Промежуточная аттестация. Для проведения промежуточной аттестации по дисциплине используются компьютерные классы, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета, и/или учебные аудитории, укомплектованные мебелью и техническими средствами обучения.

Самостоятельная работа. Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде университета. Для организации самостоятельной работы обучающихся используются: компьютерные классы университета; библиотека (медиазал), имеющая места для обучающихся, оснащенные компьютерами с доступом к базам данных и сети «Интернет».

Электронная информационно-образовательная среда университета (ЭИОС). Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронной информационно-образовательной среде университета (ЭИОС) http://sdo.tolgas.ru/ из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети «Интернет», как на территории университета, так и вне ее.

ЭИОС университета обеспечивает:

доступ к учебным планам, рабочим программам дисциплин (модулей), программам практик, электронным учебным изданиям и электронным образовательным ресурсам, указанным в рабочих программах дисциплин (модулей), программах практик;

формирование электронного портфолио обучающегося, в том числе сохранение его работ и оценок за эти работы.

В случае реализации образовательной программы с применением электронного обучения, дистанционных образовательных технологий ЭИОС дополнительно обеспечивает:

фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения образовательной программы;

проведение учебных занятий, процедур оценки результатов обучения, реализация которых предусмотрена с применением электронного обучения, дистанционных образовательных технологий;

взаимодействие между участниками образовательного процесса, в том числе синхронное и (или) асинхронное взаимодействия посредством сети "Интернет".

7. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБУЧЕНИЯ ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

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

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла; в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации;
- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации;
- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

8. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ (ФОНД ОЦЕНОЧНЫХ СРЕДСТВ) ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Для оценки знаний, умений, навыков и уровня сформированности компетенции по дисциплине применяется балльно-рейтинговая система контроля и оценки успеваемости студентов. В основу балльно-рейтинговой системы положены принципы, в соответствии с которыми формирование рейтинга студента осуществляется в ходе текущего контроля успеваемости. Максимальное количество баллов в семестре – 100.

Шкала оценки результатов освоения дисциплины, сформированности результатов обучения

Форма проведения промежуточной аттестации	**Шкалы оценки уровня сформированности результатов обучения**		**Шкала оценки уровня освоения дисциплины**		
	Уровневая шкала оценки компетенций	100 бальная шкала, %	100 бальная шкала, %	5-балльная шкала, дифференцированная оценка/балл	недифференцированная оценка
экзамен	допороговый	ниже 61	ниже 61	«неудовлетворительно» / 2	не зачтено
	пороговый	61-85,9	61-69,9	«удовлетворительно» / 3	зачтено
			70-85,9	«хорошо» / 4	зачтено
	повышенный	86-100	86-100	«отлично» / 5	зачтено

По итогам текущей успеваемости студенту может быть выставлена оценка по промежуточной аттестации в соответствии за набранными за семестр баллами (по накопительному рейтингу). Студентам, набравшим в ходе текущего контроля успеваемости по дисциплине от 61 до 100 баллов и выполнившим все обязательные виды запланированных учебных занятий, по решению преподавателя без прохождения промежуточной аттестации выставляется оценка в соответствии со шкалой оценки результатов освоения дисциплины.

***Результат обучения считается сформированным (повышенный уровень)**, если теоретическое содержание курса освоено полностью; при устных собеседованиях студент исчерпывающе, последовательно, четко и логически стройно излагает учебный материал; свободно справляется с задачами, вопросами и другими видами заданий, требующих применения знаний, использует в ответе дополнительный материал; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий, качество их выполнения оценено числом баллов от 86 до 100, что соответствует повышенному уровню сформированности результатов обучения.*

***Результат обучения считается сформированным (пороговый уровень)**, если теоретическое содержание курса освоено полностью; при устных собеседованиях студент последовательно, четко и логически стройно излагает учебный материал; справляется с задачами, вопросами и другими видами заданий, требующих применения знаний; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий, качество их выполнения оценено числом баллов от 61 до 85,9, что соответствует пороговому уровню сформированности результатов обучения.*

***Результат обучения считается несформированным**, если студент при выполнении заданий не демонстрирует знаний учебного материала, допускает ошибки, неуверенно, с большими затруднениями выполняет задания, не демонстрирует необходимых умений, качество выполненных заданий не соответствует установленным требованиям, качество их выполнения оценено числом баллов ниже 61, что соответствует допороговому уровню.*

Формы текущего контроля успеваемости

Формы текущего контроля	Количество контрольных точек	Баллов за 1 точку	Макс. балл
Устный опрос	3	5	15
Решение практических заданий	8	6	48
Тестирование по темам курса	2	8	16
Доклад/сообщение	3	7	21
Итого			**100 баллов**

Система оценивания представлена в электронном учебном курсе по дисциплине http://sdo.tolgas.ru/.

8.2. Типовые контрольные задания или иные материалы для ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

8.2.1. Типовые задания к практическим (лабораторным) занятиям

1. Сравнительный анализ классов средств защиты программного обеспечения.
2. Установка и настройка средства защиты информации от несанкционированного доступа.
3. Применение криптографического средства защиты информации для контроля целостности ПО.
4. Настройка средства контроля целостности программного обеспечения.
5. Установка, настройка и обновление антивирусного средства защиты.
6. Настройка системы обнаружения вторжений для защиты программного обеспечения.
7. Обслуживание и контроль работоспособности средств защиты программного обеспечения.
8. Оценка эффективности установленных средств защиты программного обеспечения.

8.2.2. Типовые тестовые задания для текущего контроля

Правильные варианты ответов выделены жирным шрифтом.

1. Средство защиты информации, предназначенное для разграничения прав пользователей на доступ к ресурсам компьютера, называется:

А) СЗИ от НСД

Б) антивирусом

В) архиватором

Г) файловым менеджером

2. Метод обнаружения вредоносного ПО, основанный на сравнении программного кода с базой известных образцов, называется:

А) эвристическим анализом

Б) сигнатурным анализом

В) поведенческим анализом

Г) статистическим анализом

3. Система, предназначенная для автоматического обнаружения и блокирования сетевых атак в реальном времени, называется:

А) IDS

Б) IPS

В) DLP

Г) VPN

4. Средство защиты, обеспечивающее контроль неизменности программного обеспечения в процессе эксплуатации, называется:

А) средством контроля целостности

Б) средством резервного копирования

В) межсетевым экраном

Г) архиватором

5. Технология изолированного выполнения потенциально опасного программного кода для анализа его поведения называется:

А) виртуализацией

Б) sandboxing (песочницей)

В) шифрованием

Г) архивированием

6. Регулярное пополнение базы данных известных угроз антивирусного средства защиты называется:

А) обновлением сигнатурных баз

Б) дефрагментацией

В) резервным копированием

Г) форматированием

7. Класс средств защиты, обеспечивающих расширенное обнаружение и реагирование на угрозы на конечных узлах, обозначается аббревиатурой:

А) EDR

Б) DBMS

В) API

Г) HTML

8. Оценка соответствия применяемых средств защиты установленным требованиям и определение их результативности называется:

А) оценкой эффективности средств защиты

Б) резервным копированием

В) обфускацией

Г) дефрагментацией

Темы докладов/сообщений

1. Классификация средств защиты программного обеспечения.

2. Средства защиты программного обеспечения от несанкционированного доступа (СЗИ от НСД).

3. Криптографические средства защиты программного обеспечения: назначение и характеристики.

4. Средства контроля целостности программного обеспечения.

5. Средства обнаружения и предотвращения вторжений (IDS/IPS) для защиты программного обеспечения.

Вопрос для устного опроса

1. Порядок установки средств защиты информации от несанкционированного доступа в соответствии с эксплуатационной документацией.

2. Настройка параметров работы средств защиты программного обеспечения.

3. Порядок обслуживания и сопровождения средств защиты программного обеспечения.

4. Требования к персоналу, осуществляющему эксплуатацию средств защиты программного обеспечения.

8.3. Типовые контрольные задания или иные материалы для проведения ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Форма проведения промежуточной аттестации по дисциплине: экзамен (по результатам накопительного рейтинга или в форме компьютерного тестирования).

Устно-письменная форма по вопросам к экзамену предполагается, как правило, для сдачи академической задолженности.

Перечень вопросов для подготовки к экзамену

ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности

1. Классификация средств защиты программного обеспечения.

2. Средства защиты программного обеспечения от несанкционированного доступа (СЗИ от НСД).

3. Криптографические средства защиты программного обеспечения: назначение и характеристики.

4. Средства контроля целостности программного обеспечения.

5. Средства обнаружения и предотвращения вторжений (IDS/IPS) для защиты программного обеспечения.

6. Антивирусные средства защиты программного обеспечения: принципы работы, классификация.

7. Средства защиты программного обеспечения от эксплуатации уязвимостей (EDR, sandboxing).

8. Технические средства контроля эффективности применяемых мер защиты программного обеспечения.

9. Оценка достоинств и недостатков различных классов средств защиты программного обеспечения.

10. Отечественные сертифицированные средства защиты программного обеспечения.

ПК-1. Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации

1. Порядок установки средств защиты информации от несанкционированного доступа в соответствии с эксплуатационной документацией.

2. Настройка параметров работы средств защиты программного обеспечения.

3. Порядок обслуживания и сопровождения средств защиты программного обеспечения.

4. Требования к персоналу, осуществляющему эксплуатацию средств защиты программного обеспечения.

5. Порядок обновления баз сигнатур и правил средств защиты программного обеспечения.

6. Настройка политик безопасности средств защиты от несанкционированного доступа.

7. Настройка средств антивирусной защиты программного обеспечения.

8. Настройка систем обнаружения вторжений для защиты программного обеспечения.

9. Контроль работоспособности установленных средств защиты программного обеспечения.

10. Устранение неисправностей средств защиты программного обеспечения в процессе эксплуатации.