Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Выборнова Любовь Алексеевна
Должность: Ректор
Дата подписания: 30.10.2026 13:49:29
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

«Защита 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 «Защита 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 о методах и средствах защиты программного обеспечения от угроз безопасности информации;

– формирование умения применять программные, программно-аппаратные и технические средства защиты информации, в том числе криптографические, при разработке и эксплуатации программного обеспечения;

– формирование навыков установки, настройки и обслуживания 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»	Знает: – основные характеристики, достоинства и недостатки средств криптографической и технической защиты программного обеспечения Умеет: – применять средства криптографической защиты программного обеспечения от несанкционированного доступа и модификации Владеет: – навыками применения средств криптографической и технической защиты программного обеспечения	
ПК-1. Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том	ИПК-1.1. Устанавливает, настраивает и обслуживает программное обеспечение, программно-аппаратные и	Знает: – порядок установки, настройки и обслуживания средств защиты программного обеспечения в соответствии с технической документацией Умеет:	06.032 Специалист по безопасности компьютерных систем и сетей

числе криптографических) и технических средств защиты информации	технические средства защиты информации с соблюдением требований по защите информации ИПК-1.2. Умеет устанавливать программное обеспечение в соответствии с технической документацией, выполнять настройку параметров работы программного обеспечения, включая системы управления базами данных и средства электронного документооборота, формулировать правила безопасной эксплуатации	– устанавливать и настраивать средства защиты программного обеспечения с соблюдением требований по защите информации Владеет: – навыками обслуживания программных и программно-аппаратных средств защиты программного обеспечения	

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

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

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1. Объем и структура дисциплины

Общая трудоёмкость дисциплины составляет **6 з.е. (216 час.)**, их распределение по видам работ представлено в таблице.

Виды учебных занятий и работы обучающихся	**Трудоемкость, час**		
	всего	**___3_ семестр**	**__4__ семестр**
Общая трудоемкость дисциплины, час	**216**	**144**	**108**
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего), в т.ч.:	**156 / 88**	**84 / 36**	**72 /52**
занятия лекционного типа (лекции)	70 / 40	42 / 18	28 / 22
занятия семинарского типа (семинары, практические занятия, практикумы, коллоквиумы и иные аналогичные занятия)	70 / 40	42 / 18	28 / 22
лабораторные работы	16 / 8	- / -	16 / 8
Самостоятельная работа всего, в т.ч.:	**69 / 115**	**60 / 68**	**9 /47**
Самоподготовка по темам (разделам) дисциплины	- / -	- / -	- / -
Выполнение курсового проекта /курсовой работы	36 / 36	- / -	36 / 36
Контроль (часы на экзамен, зачет)	**27 / 13**	**- / 4**	**27 / 9**
Промежуточная аттестация		**зачет**	**Экзамен/ защита КР/КП**

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		
3 семестр						
ОПК-9 ИОПК-9.1	**ТЕМА 1. УГРОЗЫ БЕЗОПАСНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ (3 СЕМЕСТР)**	11/4				Устный опрос
	Основное содержание: 1. Понятие безопасности программного обеспечения (ПО). 2. Классификация угроз безопасности ПО: несанкционированное копирование, модификация, реверс-инжиниринг. 3. Жизненный цикл ПО и этапы внедрения угроз.					
	Лабораторная 1. Исследование методов обфускации и деобфускации кода		2/1			Практическое задание
	Практическое занятие № 1. Анализ угроз безопасности типового программного продукта			11/4		Практическое задание
	Самостоятельная работа				5/17	Самостоятельное изучение методических материалов
ОПК-9 ИОПК-9.1	**ТЕМА 2. ВРЕДОНОСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ (3 СЕМЕСТР)**	11/4				Устный опрос / тестирование
	Основное содержание: 1. Классификация вредоносного программного обеспечения					

	(вирусы, черви, трояны, шифровальщики). 2. Методы распространения и заражения вредоносным ПО. 3. Признаки заражения и методы обнаружения вредоносного ПО.					
	Лабораторная 2 Анализ бинарных файлов и поиск уязвимостей		2/1			Практическое задание
	Практическое занятие № 2. Анализ признаков заражения программного обеспечения вредоносным кодом			11/4		Практическое задание
	Самостоятельная работа				5/17	Самостоятельное изучение методических материалов
ОПК-9 ИОПК-9.2	**ТЕМА 3. ЗАЩИТА ПО ОТ НЕСАНКЦИОНИРОВАННОГО КОПИРОВАНИЯ И МОДИФИКАЦИИ (3 СЕМЕСТР)**	10/4				
	Основное содержание: 1. Методы защиты программного обеспечения от несанкционированного копирования. 2. Методы защиты программного обеспечения от несанкционированной модификации. 3. Технологии лицензирования и активации программного обеспечения.					
	Лабораторная 3 Исследование механизмов переполнения буфера		2/1			Практическое задание
	Практическое занятие № 3. Анализ методов защиты ПО от копирования и модификации			10/4		Практическое задание
	Самостоятельная работа				4/17	Самостоятельное изучение методических материалов
ОПК-9 ИОПК-9.2	**ТЕМА 4. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ (3 СЕМЕСТР)**	10/4				Доклад/сообщение

	Основное содержание: 1. Применение криптографических методов для защиты программного кода. 2. Электронная подпись программного обеспечения. 3. Средства контроля целостности программного обеспечения.					
	Лабораторная 4 Создание и обнаружение программ-закладок и вирусов		2/1			Практическое задание
	Практическое занятие № 4. Применение электронной подписи для контроля целостности программного обеспечения			10/4		Практическое задание
	Самостоятельная работа				4/17	Самостоятельное изучение методических материалов
4 семестр						
ПК-1 ИПК-1.1	**ТЕМА 5. БЕЗОПАСНАЯ РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ (4 СЕМЕСТР)**	7/5				Устный опрос
	Основное содержание: 1. Понятие безопасного жизненного цикла разработки ПО (Secure SDLC). 2. Требования безопасности на этапах проектирования, разработки, тестирования ПО. 3. Стандарты и методики безопасной разработки программного обеспечения.					
	Лабораторная 5 Применение криптографических методов защиты ПО		2/1			Практическое задание
	Практическое занятие № 5. Анализ требований безопасной разработки для типового программного проекта			7/12		Практическое задание
	Самостоятельная работа				4/12	Самостоятельное изучение методических материалов

ПК-1 ИПК-1.2	**ТЕМА 6. СТАТИЧЕСКИЙ И ДИНАМИЧЕСКИЙ АНАЛИЗ БЕЗОПАСНОСТИ ПО (4 СЕМЕСТР)**	7/5				
	Основное содержание: 1. Методы статического анализа безопасности программного кода. 2. Методы динамического анализа безопасности программного обеспечения (fuzzing, отладка). 3. Инструментальные средства анализа безопасности ПО.					
	Лабораторная 6 Исследование средств защиты от отладки и реверса		2/1			Практическое задание
	Практическое занятие № 6. Проведение статического анализа безопасности программного кода с использованием инструментальных средств			7/12		Практическое задание
	Самостоятельная работа				4/12	Самостоятельное изучение методических материалов
ПК-1 ИПК-1.1, ИПК-1.2	**ТЕМА 7. УЯЗВИМОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ (4 СЕМЕСТР)**	7/5				
	Основное содержание: 1. Классификация уязвимостей программного обеспечения. 2. Методы поиска и устранения уязвимостей. 3. Реестр уязвимостей и оценка их критичности (CVE, CVSS).					
	Лабораторная 7 Анализ стойкости систем лицензирования и активации		2/1			Практическое задание
	Практическое занятие № 7. Поиск и анализ уязвимостей типового программного обеспечения			7/12		Практическое задание / тестирование
	Самостоятельная работа				4/12	Самостоятельное изучение методических материалов
ПК-1	**ТЕМА 8. УСТАНОВКА, НАСТРОЙКА И**	7/5				

ИПК-1.1	**ОБСЛУЖИВАНИЕ СРЕДСТВ ЗАЩИТЫ ПО (4 СЕМЕСТР)**					
	Основное содержание: 1. Порядок установки и настройки средств защиты программного обеспечения в соответствии с технической документацией. 2. Обслуживание и сопровождение средств защиты программного обеспечения. 3. Особенности защиты программного обеспечения отечественного производства.					
	Лабораторная 8 Аудит безопасности веб-приложений и API		2/1			Практическое задание
	Практическое занятие № 8. Установка и настройка средств защиты типового программного обеспечения			7/12		Практическое задание
	Самостоятельная работа				3/12	Самостоятельное изучение методических материалов
	Выполнение курсовой работы				36/36	
	ИТОГО по дисциплине	**70/40**	**16/8**	**70/40**	**69/115**	

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/.

4.6. Методические указания для выполнения курсового проекта / работы

Выполнение курсового проекта/ работы способствует лучшему освоению обучающимися учебного материала, формирует практический опыт и умения по изучаемой дисциплине, способствует формированию у обучающихся готовности к самостоятельной профессиональной деятельности, является этапом к выполнению выпускной квалификационной работы.

Типовые темы курсовых работ

Курсовая работа выполняется в 4 семестре и предполагает анализ и разработку предложений по защите программного обеспечения конкретного типа. Примерные темы курсовых работ:

1. Разработка методов защиты программного обеспечения от несанкционированного копирования.

2. Анализ и устранение уязвимостей веб-приложения.

3. Исследование методов обфускации программного кода.

4. Разработка средства контроля целостности программного обеспечения.

5. Анализ угроз безопасности мобильного приложения и разработка мер защиты.

6. Исследование методов защиты программного обеспечения от реверс-инжиниринга.

7. Разработка политики безопасной разработки программного обеспечения для организации.

8. Сравнительный анализ инструментальных средств статического анализа кода.

9. Разработка методики тестирования программного обеспечения на устойчивость к атакам.

10. Исследование применения электронной подписи для защиты программного обеспечения.

- Цели и задачи курсового проектирования
- Выбор темы курсового проектирования
- Организация, выполнение и руководство курсовым проектированием
- Структура и содержание курсового проекта / работы. Методические указания по выполнению основных разделов
- Требования к оформлению курсового проекта / работы
- Порядок сдачи и защиты курсового проекта / работы

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

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

3. Артюшенко, В. М. Защита программного обеспечения от несанкционированного использования : учебное пособие / В. М. Артюшенко. – Москва : Горячая линия – Телеком. – Текст : электронный.

Дополнительная литература:

4. Скляров, Д. В. Искусство защиты и взлома информации / Д. В. Скляров. – Санкт-Петербург : БХВ-Петербург. – Текст : непосредственный.

5. Крис, К. Тестирование безопасности программного обеспечения / К. Крис. – Москва : ДМК Пресс. – Текст : непосредственный.

6. Учебно-методическое пособие по дисциплине «Защита программного обеспечения» : для студентов направления подготовки 10.03.01 «Информационная безопасность» / Поволж. гос. ун-т сервиса (ФГБОУ ВО «ПВГУС») ; сост.: Ю. С. Мунирова. – Тольятти : ПВГУС. – Текст : электронный.

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

1. Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России) : сайт. – URL: https://fstec.ru – Текст : электронный.

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

3. База данных уязвимостей NVD/CVE : сайт. – URL: https://nvd.nist.gov – 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.

6. Электронно-библиотечная система Znanium.com : сайт / ООО «ЗНАНИУМ». – Москва. – URL: https://znanium.com/ – 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	Microsoft Windows	из внутренней сети университета (лицензионный договор)
2	Среда разработки программного обеспечения (IDE)	из компьютерных классов университета (свободно распространяемое программное обеспечение)

3	Инструментальные средства статического анализа кода	из компьютерных классов университета (свободно распространяемое программное обеспечение)
4	Антивирусное программное обеспечение отечественного производства	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
Зачет Экзамен/Защита КП	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	4	5	20
Решение практических (лабораторных) заданий	8	6	48
Тестирование по темам курса	2	8	16
Доклад/сообщение	2	8	16
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. Анализ угроз безопасности типового программного продукта.

2. Анализ признаков заражения программного обеспечения вредоносным кодом.

3. Анализ методов защиты ПО от копирования и модификации.

4. Применение электронной подписи для контроля целостности программного обеспечения.

5. Анализ требований безопасной разработки для типового программного проекта.

6. Проведение статического анализа безопасности программного кода с использованием инструментальных средств.

7. Поиск и анализ уязвимостей типового программного обеспечения.

8. Установка и настройка средств защиты типового программного обеспечения.

Список лабораторных работ

1. Исследование методов обфускации и деобфускации кода

Цель: Изучение способов защиты программного кода от анализа.

Описание: Студенты применяют методы переименования идентификаторов, запутывания управляющих конструкций и шифрования строк. Затем они проводят анализ и восстановление исходной структуры кода с помощью деобфускаторов.

2. Анализ бинарных файлов и поиск уязвимостей

Цель: Освоение инструментов статического и динамического анализа.

Описание: С использованием дебаггеров и дизассемблеров исследуется скомпилированный код программы. Находятся логические ошибки, незащищенные функции и потенциальные точки для внедрения стороннего кода.

3. Исследование механизмов переполнения буфера

Цель: Изучение уязвимостей стека и методов их эксплуатации.

Описание: Создается учебная программа с уязвимостью переполнения буфера. Проводится атака с перезаписью адреса возврата, после чего изучаются методы предотвращения таких сбоев (например, технологии защиты стека DEP и ASLR).

4. Создание и обнаружение программ-закладок и вирусов

Цель: Понимание принципов работы вредоносного ПО.

Описание: Рассматриваются базовые алгоритмы внедрения вредоносного кода в легитимные файлы. Студенты настраивают сигнатурный и эвристический анализ для поиска этих элементов в изолированной среде.

5. Применение криптографических методов защиты ПО

Цель: Защита целостности и конфиденциальности приложений.

Описание: Реализуется проверка цифровой подписи исполняемого файла, шифрование конфигурационных файлов и защита критически важных участков кода с помощью симметричных и асимметричных алгоритмов.

6. Исследование средств защиты от отладки и реверса

Цель: Знакомство с методами противодействия анализу (Anti-Debugging / Anti-Analysis).

Описание: В программный продукт внедряются проверки на наличие запущенных отладчиков, виртуальных машин или песочниц. Студенты учатся обходить эти защитные механизмы.

7. Анализ стойкости систем лицензирования и активации

Цель: Изучение систем защиты от пиратства.

Описание: Исследуются механизмы проверки ключей продукта, привязка софта к аппаратным идентификаторам ПК (жесткому диску или процессору). Проводится анализ надежности таких проверок.

8. Аудит безопасности веб-приложений и API

Цель: Защита программного обеспечения, работающего в клиент-серверной архитектуре.

Описание: Проверяется защищенность интерфейсов программы от распространенных угроз (включая инъекции и несанкционированный доступ). Разрабатываются рекомендации по устранению найденных дыр в безопасности.

8.2.2. Типовые тестовые задания для текущего контроля

Правильные варианты ответов выделены жирным шрифтом.

1. Процесс намеренного искажения работы программного обеспечения без разрешения правообладателя называется:

А) несанкционированной модификацией

Б) сертификацией

В) лицензированием

Г) резервным копированием

2. Программа, скрытно устанавливающаяся в системе и предоставляющая злоумышленнику удаленный доступ, называется:

А) файловым вирусом

Б) троянской программой

В) программой-упаковщиком

Г) отладчиком

3. Метод анализа безопасности программного кода, выполняемый без запуска программы, называется:

А) динамическим анализом

Б) статическим анализом

В) нагрузочным тестированием

Г) регрессионным тестированием

4. Уникальный идентификатор известной уязвимости программного обеспечения в международной базе данных обозначается аббревиатурой:

А) CVE

Б) DLP

В) VPN

Г) SIEM

5. Технология преобразования программного кода с целью затруднения его анализа при сохранении функциональности называется:

А) компиляцией

Б) обфускацией

В) декомпиляцией

Г) виртуализацией

6. Средство, предназначенное для аппаратной защиты программного обеспечения от несанкционированного запуска, называется:

А) электронным ключом (токеном)

Б) межсетевым экраном

В) антивирусом

Г) архиватором

7. Жизненный цикл разработки программного обеспечения с интегрированными требованиями безопасности на всех этапах называется:

А) Waterfall

Б) Secure SDLC

В) Scrum

Г) Kanban

8. Оценка критичности уязвимости программного обеспечения по стандартизированной шкале выполняется с использованием системы:

А) CVSS

Б) ГОСТ Р ИСО 9001

В) ITIL

Г) ISO 14001

Темы докладов/сообщений

1. Понятие и виды угроз безопасности программного обеспечения.
2. Классификация вредоносного программного обеспечения.
3. Методы и средства защиты программного обеспечения от несанкционированного копирования.
4. Методы и средства защиты программного обеспечения от несанкционированной модификации.

Вопросы для устного опроса

1. Разработка методов защиты программного обеспечения от несанкционированного копирования.
2. Анализ и устранение уязвимостей веб-приложения.
3. Исследование методов обфускации программного кода.

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

Форма проведения промежуточной аттестации по дисциплине: зачет и экзамен/ *защита курсового проекта (курсовой работы)*.

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

Защита курсового проекта/ работы. *Результаты защиты курсового проекта/ работы выставляются по пятибалльной системе оценивания ("отлично", "хорошо", "удовлетворительно", "неудовлетворительно") с обязательным проставлением количества баллов, набранных в соответствии с балльно-рейтинговой системой (по стобалльной шкале).*

Типовые темы курсовых работ

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

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

Курсовая работа выполняется в 4 семестре и предполагает анализ и разработку предложений по защите программного обеспечения конкретного типа. Примерные темы курсовых работ:

1. Разработка методов защиты программного обеспечения от несанкционированного копирования.
2. Анализ и устранение уязвимостей веб-приложения.
3. Исследование методов обфускации программного кода.
4. Разработка средства контроля целостности программного обеспечения.
5. Анализ угроз безопасности мобильного приложения и разработка мер защиты.
6. Исследование методов защиты программного обеспечения от реверс-инжиниринга.
7. Разработка политики безопасной разработки программного обеспечения для организации.
8. Сравнительный анализ инструментальных средств статического анализа кода.
9. Разработка методики тестирования программного обеспечения на устойчивость к атакам.
10. Исследование применения электронной подписи для защиты программного обеспечения.

Перечень вопросов для подготовки к зачету

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

1. Средства защиты программного обеспечения от статического и динамического анализа.
2. Технологии обфускации программного кода.
3. Средства электронной подписи программного обеспечения.
4. Защита программного обеспечения от отладки и трассировки.

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

1. Уязвимости программного обеспечения: классификация и методы устранения.
2. Средства контроля целостности программного обеспечения.
3. Порядок сертификации средств защиты информации, встроенных в программное обеспечение.

4. Особенности защиты программного обеспечения отечественного производства.

5. Обслуживание и сопровождение средств защиты программного обеспечения в процессе эксплуатации.

Перечень вопросов для подготовки к экзамену

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

1. Понятие и виды угроз безопасности программного обеспечения.
2. Классификация вредоносного программного обеспечения.
3. Методы и средства защиты программного обеспечения от несанкционированного копирования.
4. Методы и средства защиты программного обеспечения от несанкционированной модификации.
5. Криптографические методы защиты программного обеспечения.
6. Аппаратные средства защиты программного обеспечения (электронные ключи, токены).

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 и настройки средств защиты программного обеспечения в соответствии с технической документацией.
2. Требования безопасной разработки программного обеспечения (Secure Software Development Lifecycle).
3. Методы статического анализа безопасности программного кода.
4. Методы динамического анализа безопасности программного обеспечения.
5. Тестирование программного обеспечения на устойчивость к атакам.