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:
c3b3b9c625f6c113afa2a2c42baff9e0ba38b7c8

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

«Кибербезопасность»

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 *«Кибербезопасность»* 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)*		*(подпись)*

РПД обсуждена на заседании Высшей школы интеллектуальных систем и кибертехнологий

«23» _05_ 2025_ г., протокол № _10_

Директор Высшей школы интеллектуальных систем и кибертехнологий		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

Целью освоения дисциплины является:

– формирование у обучающихся универсальных компетенций, направленных на развитие навыков системного и критического мышления в области поиска, анализа и обработки научно-технической информации в сфере информационных технологий;

– формирование у обучающихся профессиональных компетенций, необходимых для решения задач профессиональной деятельности в области обеспечения кибербезопасности, связанных с инсталляцией, тестированием и использованием программных и аппаратных средств защиты информации.

– формирование у обучающихся универсальных компетенций, *направленных на развитие навыков системного и критического мышления*

– *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
УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	**ИУК-1.1.** Осуществляет поиск, анализирует и обрабатывает научно-техническую информацию в ИТ-сфере, в том числе в области кибербезопасности	**Знает:** основные источники научно-технической информации в области кибербезопасности; методы поиска, критического анализа и систематизации информации по вопросам защиты информации **Умеет:** находить, анализировать и обрабатывать научно-техническую информацию в ИТ-сфере при решении задач обеспечения кибербезопасности **Владеет:** навыками системного поиска и критической оценки научно-технической информации в области кибербезопасности	
ПК-2 Способен применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и	**ИПК-2.1.** Противодействует угрозам безопасности информации с использованием встроенных средств защиты информации	**Знает:** состав, назначение и принципы функционирования программных средств защиты информации (антивирусное ПО, средства криптографической защиты, межсетевые экраны, системы обнаружения вторжений) **Умеет:** инсталлировать и тестировать программные средства защиты информации, оценивать корректность их настройки и работы	06.032 «Специалист по безопасности компьютерных систем и сетей»

системы программирования для решения профессиональных задач		**Владеет:** навыками использования программных средств защиты информации для решения задач профессиональной деятельности	
ПК-3 Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	**ИПК-3.1.** Оценивает работоспособность применяемых средств защиты информации с использованием штатных средств и методик	**Знает:** состав, назначение и принципы функционирования аппаратных средств защиты информации (аппаратные модули доверенной загрузки, токены, аппаратные межсетевые экраны, СКЗИ) **Умеет:** инсталлировать и тестировать аппаратные средства защиты информации, оценивать корректность их настройки и работы **Владеет:** навыками использования аппаратных средств защиты информации для решения задач профессиональной деятельности	06.032 «Специалист по безопасности компьютерных систем и сетей»

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина относится к части, формируемой участниками образовательных отношений, Блока 1. Дисциплины (модули) образовательной программы (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 и семестрам 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.:	**52/24**
занятия лекционного типа (лекции)	18/12
занятия семинарского типа (практические занятия)	30/10
лабораторные работы	4/2
Самостоятельная работа всего, в т.ч.:	**65/111**
Самоподготовка по темам (разделам) дисциплины	65/111
Контроль (часы на экзамен)	**27/9**
Промежуточная аттестация	**Экзамен**

Примечание: *-/- объем часов соответственно для очной и очно-заочной формы 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	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		
УК-1: ИУК-1.1	**Тема 1. Основы кибербезопасности: понятия, цели и задачи** *Содержание лекции:* 1. Понятие кибербезопасности, информационной безопасности и защиты информации 2. Цели, задачи и объекты кибербезопасности 3. Основные направления обеспечения кибербезопасности в РФ	2/1	–	–	–	Устный опрос / тестирование
	Практическое занятие № 1. Анализ научно-технической информации по актуальным угрозам кибербезопасности	–	–	4/1	–	
	Самостоятельная работа: Изучение учебной литературы по теме, подготовка к практическому занятию	–	–	–	8/10	
УК-1: ИУК-1.1	**Тема 2. Угрозы информационной безопасности и модель нарушителя** *Содержание лекции:* 1. Классификация угроз информационной безопасности 2. Источники и каналы утечки информации 3. Модель нарушителя и модель угроз	2/1	–	–	–	Устный опрос / практическое задание

	Практическое занятие № 2. Построение модели угроз для типовой информационной системы	–	–	4/1	–	
	Самостоятельная работа: Изучение классификаторов угроз (БДУ ФСТЭК России), подготовка к занятию	–	–	–	8/10	
ПК-2: ИПК-2.1	**Тема 3. Вредоносное программное обеспечение и антивирусная защита** *Содержание лекции:* 1. Классификация вредоносного программного обеспечения 2. Механизмы распространения и заражения 3. Принципы работы антивирусных программных средств	2/1	–	–	–	Отчет по лабораторной работе / тестирование
	Лабораторная работа № 1. Инсталляция и тестирование антивирусного программного средства защиты информации	–	2/1	–	–	
	Практическое занятие № 3. Настройка политик антивирусной защиты	–	–	4/1	–	
	Самостоятельная работа: Изучение отечественных антивирусных решений, подготовка отчета по лабораторной работе	–	–	–	8/10	
ПК-2: ИПК-2.1	**Тема 4. Криптографические методы защиты информации** *Содержание лекции:* 1. Симметричные и асимметричные криптографические алгоритмы 2. Электронная подпись и хеширование 3. Отечественные средства	2/1	–	–	–	Практическое задание / тестирование

	криптографической защиты информации (СКЗИ)					
	Практическое занятие № 4. Использование программных средств криптографической защиты информации	–	–	4/1	–	
	Самостоятельная работа: Изучение ГОСТ Р 34.10-2018, ГОСТ Р 34.11-2018, подготовка к занятию	–	–	–	8/10	
ПК-3: ИПК-3.1	**Тема 5. Сетевая безопасность: межсетевые экраны, VPN, IDS/IPS** *Содержание лекции:* 1. Архитектура защищенных сетей 2. Программные и аппаратные межсетевые экраны 3. Технологии VPN, системы обнаружения и предотвращения вторжений (IDS/IPS)	2/1	–	–	–	Отчет по лабораторной работе / практическое задание
	Лабораторная работа № 2. Инсталляция и тестирование аппаратно-программного средства сетевой защиты (межсетевого экрана)	–	2/1	–	–	
	Практическое занятие № 5. Настройка правил межсетевого экранирования	–	–	4/1	–	
	Самостоятельная работа: Изучение документации по настройке средств сетевой защиты, подготовка отчета	–	–	–	8/10	
ПК-2, ИПК-2.1; **ПК-3:** ИПК-3.1	**Тема 6. Идентификация, аутентификация и управление доступом** *Содержание лекции:* 1. Методы и средства идентификации и аутентификации 2. Аппаратные средства	2/1	–	–	–	Практическое задание / устный опрос

	аутентификации (токены, смарт-карты) 3. Модели разграничения доступа (дискреционная, мандатная, ролевая)					
	Практическое занятие № 6. Настройка программных и аппаратных средств разграничения доступа	–	–	4/1	–	
	Самостоятельная работа: Изучение стандартов управления доступом, подготовка к занятию	–	–	–	8/10	
ПК-2, ИПК-2.1; **ПК-3:** ИПК-3.1	**Тема 7. Тестирование и эксплуатация программных и аппаратных средств защиты информации** *Содержание лекции:* 1. Методика тестирования средств защиты информации 2. Оценка эффективности функционирования программных и аппаратных средств защиты 3. Порядок эксплуатации и сопровождения средств защиты информации	3/1	–	–	–	Практическое задание
	Практическое занятие № 7. Комплексное тестирование программно-аппаратного комплекса защиты информации	–	–	3/1	–	
	Самостоятельная работа: Подготовка отчета по результатам тестирования средств защиты информации	–	–	–	9/10	
УК-1, ИУК-1.1; **ПК-2,** ИПК-2.1; **ПК-3:** ИПК-3.1	**Тема 8. Нормативно-правовое обеспечение кибербезопасности и управление инцидентами** *Содержание лекции:* 1. Нормативно-правовые акты РФ в области защиты	3/1	–	–	–	Практическое задание / тестирование

	информации (ФЗ-149, ФЗ-152, приказы ФСТЭК и ФСБ России) 2. Международные и национальные стандарты (ISO/IEC 27001, ГОСТ Р ИСО/МЭК 27001) 3. Организация реагирования на инциденты информационной безопасности					
	Практическое занятие № 8. Разработка плана реагирования на инцидент информационной безопасности	–	–	3/1	–	
	Самостоятельная работа: Изучение нормативно-правовых актов, подготовка к экзамену	–	–	–	8/10	
	ИТОГО	**18/12**	**4/2**	**30/10**	**65/111**	

Примечание: *-/- объем часов соответственно для очной и очно-заочной формы 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.

Преподавание дисциплины ведется с применением следующих видов **образовательных технологий:**

– балльно-рейтинговая технология оценивания;

– электронное обучение;

– проблемное обучение;

– разбор конкретных ситуаций (кейс-технологии);

– информационные технологии: ЭИОС университета, программные и аппаратные средства защиты информации.

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.

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 понятия и принципы обеспечения кибербезопасности, обозначаются ключевые аспекты тем, а также делаются акценты на наиболее сложные и важные положения изучаемого материала.

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

В ходе лекционных занятий рекомендуется конспектирование учебного материала. Материалы лекций являются опорной основой для подготовки обучающихся к практическим занятиям, лабораторным работам и 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 лабораторных работах

Подготовку к каждой лабораторной работе студент должен начать с ознакомления с планом занятия, который отражает содержание предложенной темы. Каждая выполненная работа с оформленным отчетом по ней подлежит защите преподавателю.

При оценивании лабораторных работ учитывается следующее:

– качество выполнения работы по инсталляции, настройке и тестированию программных и аппаратных средств защиты информации и степень соответствия результатов работы заданным требованиям;

– качество оформления отчета по работе;

– качество устных ответов на контрольные вопросы при защите работы.

Лабораторные работы организуются, в том числе в форме практической подготовки, которая предусматривает участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью: инсталляцией, тестированием и использованием программных и аппаратных средств защиты информации при изучении тем 3, 5.

4.4. Методические указания для обучающихся по освоению дисциплины на практических занятиях

Практические занятия представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы дисциплины. Основной формой проведения практических занятий является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, решение практических задач, разбор кейсов, связанных с обеспечением кибербезопасности.

Практические занятия обучающихся обеспечивают:

– проверку и уточнение знаний, полученных на лекциях;

– получение умений и навыков поиска, анализа и обработки научно-технической информации, настройки программных и аппаратных средств защиты информации;

– подведение итогов занятий по рейтинговой системе, согласно технологической карте дисциплины.

4.5. 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:

1. Изучение учебной литературы по курсу.
2. Изучение нормативно-правовых актов и стандартов в области кибербезопасности.
3. Работу с ресурсами Интернет (реестр отечественного ПО, БДУ ФСТЭК России).
4. Подготовку отчетов по лабораторным работам.
5. Подготовку к тестированию по темам курса.
6. 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. Бирюков, А. А. Информационная безопасность: защита и нападение : учебное пособие / А. А. Бирюков. – Москва : ДМК Пресс.

2. Шаньгин, В. Ф. Информационная безопасность и защита информации : учебное пособие / В. Ф. Шаньгин. – Москва : ДМК Пресс.

3. Запечников, С. В. Информационная безопасность открытых систем : учебник / С. В. Запечников, Н. Г. Милославская, А. И. Толстой. – Москва : Горячая линия – Телеком.

Дополнительная литература

1. Малюк, А. А. Информационная безопасность: концептуальные и методологические основы защиты информации : учебное пособие / А. А. Малюк. – Москва : Горячая линия – Телеком.

2. Аверченков, В. И. Организационная защита информации : учебное пособие / В. И. Аверченков, М. Ю. Рытов. – Москва : Флинта.

3. ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

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

1. КонсультантПлюс : справочная правовая система : сайт. – URL: http://www.consultant.ru – Текст : электронный.

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

3. Электронно-библиотечная система Znanium.com : сайт. – URL: https://znanium.com/ – Режим доступа: для авториз. пользователей. – Текст : электронный.

4. Банк данных угроз безопасности информации ФСТЭК России : сайт. – URL: https://bdu.fstec.ru – Текст : электронный.

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

6. eLIBRARY.RU : научная электронная библиотека : сайт. – URL: https://elibrary.ru – 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:

№	Наименование	Условия доступа
1	Microsoft Windows / отечественная операционная система (Astra Linux)	из внутренней сети университета (лицензионный договор)
2	Microsoft Office / LibreOffice	из внутренней сети университета (лицензионный договор)
3	Kaspersky Endpoint Security (отечественное антивирусное ПО)	из внутренней сети университета (лицензионный договор)
4	КриптоПро CSP (СКЗИ)	из внутренней сети университета (лицензионный договор)
5	СДО MOODLE	из любой точки, в которой имеется доступ к сети Интернет (лицензионный договор)
6	КонсультантПлюс	из внутренней сети университета (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 типа. Учебные аудитории укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации.

Лабораторные работы. Для проведения лабораторных работ используется учебная аудитория «Лаборатория информационной безопасности», оснащенная компьютерной техникой с установленным программным и аппаратным обеспечением защиты информации (антивирусное ПО, СКЗИ, программные и аппаратные межсетевые экраны).

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; индивидуальные консультации и задания;

– для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика;

– 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**	**Количество баллов за 1 контр. точку**	**Макс. кол-во баллов**
Устный опрос / тестирование по темам лекционных занятий	4	5	20
Практические задания	8	5	40
Отчеты по лабораторным работам	4	10	40
Итого по дисциплине			**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 занятиям

Практическое занятие № 2. Построение модели угроз для типовой информационной системы

Задание: на основе банка данных угроз безопасности информации ФСТЭК России постройте модель угроз для заданной информационной системы (веб-сервер организации). Определите не менее 5 актуальных угроз, укажите источники угроз, объекты воздействия и возможные последствия реализации угроз.

Практическое занятие № 5. Настройка правил межсетевого экранирования

Задание: сформулируйте и обоснуйте набор правил межсетевого экрана для сегмента корпоративной сети (разрешенные/запрещенные направления и протоколы), обеспечивающий минимально необходимый уровень доступа при сохранении работоспособности типовых сервисов (веб, почта, DNS).

8.2.2. Типовые задания к лабораторным работам

Лабораторная работа № 1. Инсталляция и тестирование антивирусного программного средства защиты информации

Задание: установите антивирусное программное средство защиты информации, настройте политики проверки и обновления баз, проведите тестовую проверку на наличие вредоносного ПО (с использованием тестового файла EICAR), оформите отчет с описанием результатов тестирования.

Лабораторная работа № 2. Инсталляция и тестирование аппаратно-программного средства сетевой защиты

Задание: настройте программный либо аппаратный межсетевой экран согласно заданному набору правил, проведите тестирование корректности фильтрации трафика, оформите отчет с результатами тестирования.

Вопросы для устного опроса

1. Понятие кибербезопасности, информационной безопасности и защиты информации, их соотношение.
2. Цели, задачи и объекты обеспечения кибербезопасности.
3. Классификация угроз информационной безопасности.
4. Источники и каналы утечки информации.
5. Модель нарушителя и модель угроз информационной безопасности.

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 устно-письменной форме по экзаменационным билетам).

Перечень вопросов и заданий для подготовки к экзамену
УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач

1. Понятие кибербезопасности, информационной безопасности и защиты информации, их соотношение.
2. Цели, задачи и объекты обеспечения кибербезопасности.
3. Классификация угроз информационной безопасности.
4. Источники и каналы утечки информации.
5. Модель нарушителя и модель угроз информационной безопасности.
6. Нормативно-правовые акты Российской Федерации в области защиты информации (ФЗ-149, ФЗ-152, приказы ФСТЭК и ФСБ России).
7. Международные и национальные стандарты информационной безопасности (ISO/IEC 27001, ГОСТ Р ИСО/МЭК 27001).
8. Организация реагирования на инциденты информационной безопасности.
9. Методика поиска и критического анализа научно-технической информации в области кибербезопасности.

ПК-2. Способен применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач

1. Классификация вредоносного программного обеспечения.
2. Механизмы распространения и заражения вредоносным программным обеспечением.
3. Принципы работы и виды антивирусных программных средств защиты информации.
4. Порядок инсталляции и тестирования антивирусных программных средств защиты информации.
5. Симметричные криптографические алгоритмы: назначение и область применения.
6. Асимметричные криптографические алгоритмы: назначение и область применения.
7. Электронная подпись и хеширование: назначение, принципы функционирования.
8. Отечественные средства криптографической защиты информации (СКЗИ).
9. Программные межсетевые экраны: назначение, порядок инсталляции и тестирования.
10. Программные средства идентификации и аутентификации пользователей.
11. Методика тестирования программных средств защиты информации и оценки эффективности их функционирования.

ПК-3. Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно- аппаратных и технических средств защиты информации

1. Архитектура защищенных сетей: основные принципы построения.
2. Аппаратные межсетевые экраны: назначение, классификация, порядок инсталляции и тестирования.
3. Технологии VPN: назначение и принципы функционирования.
4. Системы обнаружения и предотвращения вторжений (IDS/IPS).
5. Аппаратные средства аутентификации (токены, смарт-карты): инсталляция и тестирование.

6. Модели разграничения доступа: дискреционная, мандатная, ролевая.
7. Методика тестирования аппаратных средств защиты информации и оценки эффективности их функционирования.
8. Порядок эксплуатации и сопровождения программных и аппаратных средств защиты информации.

Примерный тест для итогового тестирования

Правильный вариант ответа выделен полужирным шрифтом с подчеркиванием.

1. Кибербезопасность направлена прежде всего на обеспечение

А) конфиденциальности, целостности и доступности информации в компьютерных системах и сетях

Б) только конфиденциальности информации
В) только физической сохранности носителей информации
Г) только бесперебойной работы оборудования

2. Модель нарушителя описывает

А) предполагаемые возможности, мотивацию и уровень доступа лица, способного реализовать угрозу

Б) перечень технических средств защиты информации
В) структуру службы информационной безопасности организации
Г) порядок резервного копирования данных

3. Вирус, троян, червь и шифровальщик являются разновидностями

А) вредоносного программного обеспечения

Б) средств криптографической защиты информации
В) систем обнаружения вторжений
Г) аппаратных модулей доверенной загрузки

4. Основное назначение антивирусного программного средства защиты информации

А) обнаружение, блокирование и удаление вредоносного программного обеспечения

Б) шифрование сетевого трафика
В) разграничение прав доступа к файловой системе
Г) резервное копирование данных

5. К симметричным криптографическим алгоритмам относится

А) ГОСТ 28147-89 (Магма)

Б) RSA
В) алгоритм Диффи – Хеллмана
Г) ГОСТ Р 34.10-2018

6. Асимметричное шифрование, в отличие от симметричного, использует

А) пару ключей – открытый и закрытый

Б) один и тот же ключ для шифрования и расшифрования
В) только хеш-функции без ключей
Г) исключительно аппаратные средства

7. Электронная подпись обеспечивает

А) подтверждение авторства и целостности электронного документа

Б) ускорение передачи данных по сети
В) сжатие объема хранимой информации
Г) автоматическое резервное копирование

8. СКЗИ – это средства

А) криптографической защиты информации

Б) контроля физического доступа в помещение
В) видеонаблюдения
Г) кадрового делопроизводства

9. Межсетевой экран (файрвол) предназначен для

А) фильтрации сетевого трафика в соответствии с заданными правилами безопасности
Б) хранения резервных копий данных
В) проверки орфографии в документах
Г) управления кадровым составом организации
10. Технология VPN обеспечивает
А) создание защищенного (шифрованного) канала передачи данных поверх открытой сети
Б) ускорение работы процессора
В) автоматическое обновление операционной системы
Г) визуализацию сетевого трафика
11. Система обнаружения вторжений (IDS) в отличие от системы предотвращения вторжений (IPS)
А) только выявляет и сигнализирует о подозрительной активности, не блокируя ее автоматически
Б) всегда блокирует любую сетевую активность
В) устанавливается исключительно на аппаратном уровне
Г) не требует настройки правил
12. Аппаратный токен применяется для
А) аппаратной аутентификации пользователя
Б) увеличения объема оперативной памяти
В) охлаждения серверного оборудования
Г) печати документов
13. Дискреционная модель разграничения доступа предполагает, что
А) владелец ресурса самостоятельно определяет права доступа других субъектов к этому ресурсу
Б) права доступа определяются исключительно меткой секретности
В) доступ предоставляется на основании должностной роли пользователя
Г) доступ к ресурсу невозможно ограничить
14. Мандатная модель разграничения доступа основана на
А) сопоставлении меток конфиденциальности субъекта и объекта доступа
Б) решении владельца ресурса
В) случайном распределении прав доступа
Г) исключительно биометрических данных пользователя
15. Ролевая модель разграничения доступа (RBAC) назначает права доступа на основании
А) роли (должностной функции) пользователя в организации
Б) времени суток
В) географического местоположения пользователя
Г) объема оперативной памяти компьютера пользователя
16. Федеральный закон № 149-ФЗ регулирует отношения в области
А) информации, информационных технологий и защиты информации
Б) персональных данных исключительно медицинских учреждений
В) государственной тайны
Г) бухгалтерского учета
17. Федеральный закон № 152-ФЗ регулирует отношения в области
А) обработки и защиты персональных данных
Б) защиты государственной тайны
В) лицензирования образовательной деятельности
Г) антимонопольного регулирования
18. Стандарт ГОСТ Р ИСО/МЭК 27001 устанавливает требования к
А) системе менеджмента информационной безопасности организации
Б) бухгалтерской отчетности предприятия

В) качеству печатной продукции
Г) охране труда на производстве
19. Реагирование на инцидент информационной безопасности начинается с этапа
А) обнаружения и регистрации инцидента
Б) уничтожения всех журналов событий
В) увольнения ответственного сотрудника
Г) отключения всей организации от сети Интернет
20. Оценка эффективности функционирования средства защиты информации проводится с целью
А) подтверждения соответствия его работы установленным требованиям безопасности
Б) увеличения стоимости средства защиты
В) сокращения штата специалистов по информационной безопасности
Г) изменения дизайна пользовательского интерфейса