Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Самарский государственный технический университет»
(ФГБОУ ВО «СамГТУ»)
Филиал ФГБОУ ВО «СамГТУ» в г. Белебее Республики Башкортостан

УТВЕРЖДАЮ
Директор филиала ФГБОУ ВО «СамГТУ»
в г. Белебее Республики Башкортостан
_____ Л.М. Инаходова
25.05.2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.03.13 «Безопасность информационных технологий и систем»

Код и направление подготовки (специальность)	**09.03.02 Информационные системы и технологии**
Направленность (профиль)	**Информационные системы и технологии**
Квалификация	**Бакалавр**
Форма обучения	**Заочная**
Год начала подготовки	**2023**
Выпускающая кафедра	**Инженерные технологии**
Кафедра-разработчик	**Инженерные технологии**
Объем дисциплины, ч. / з.е.	**108 / 3**
Форма контроля (промежуточная аттестация)	**Зачет**

Белебей 2023 г.

Рабочая программа дисциплины (далее – РПД) разработана в соответствии с требованиями ФГОС ВО по направлению подготовки (специальности) 09.03.02 «Информационные системы и технологии», утвержденного приказом Министерства образования и науки РФ от 19 сентября 2017 г. № 926, и соответствующего учебного плана.

Разработчик РПД:

старший преподаватель		И.Е. Панфилова
(должность, степень, ученое звание)	(подпись)	(ФИО)

РПД рассмотрена и одобрена на заседании кафедры 25.05.2023 г., протокол № 6.

Заведующий кафедрой	к.т.н., доцент	А.А. Цынаева
	(степень, ученое звание, подпись)	(ФИО)

СОГЛАСОВАНО:

Руководитель образовательной программы	доцент, к.т.н.	З.Ф. Камальдинова
	(степень, ученое звание, подпись)	(ФИО)

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программ

Универсальные компетенции

Таблица 1

Наименование категории (группы) компетенций	Код компетенции	Наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения
не предусмотрены учебным планом				

Общепрофессиональные компетенции

Таблица 2

Код компетенции	Наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения
не предусмотрены учебным планом			

Профессиональные компетенции

Таблица 3

Код компетенции	Наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения
ПК-1	Способность выполнять концептуальное, функциональное и логическое проектирование систем среднего и крупного масштаба и сложности	**ПК-1.4** Подготавливает методики оценки на соответствие требованиям и оценивает качества готовых информационных систем	**В4 ПК-1.4** Владеть: Способностью к сбору, обработке и анализу готовых систем на соответствие требованиям
		ПК-1.7 Обеспечивает безопасность и целостность данных информационных систем и технологий	**З8 ПК-1.7** Знать: Основные понятия и определения предмета защиты информации, методическое и техническое обеспечение информационной безопасности **У6 ПК-1.7** Уметь: Применять методы и средства криптографической защиты **В7 ПК-1.7** Владеть: Способами контроля целостности информации

2. Место дисциплины (модуля) в структуре образовательной программы

Место дисциплины в структуре образовательной программы: часть, формируемая участниками образовательных отношений.

Таблица 4

Код компетенции	Предшествующие дисциплины	Параллельно осваиваемые дисциплины	Последующие дисциплины
ПК-1	Производственная практика: технологическая (проектно-технологическая) практика	Концептуальное проектирование и управление разработкой информационных систем; Документирование информационных систем; Практико-ориентированный проект; Корпоративные информационные системы	Надежность и оценка качества информационных систем; Математические основы моделирования информационных систем; Моделирование информационных процессов и систем; Эксплуатация информационных систем; Производственная практика: преддипломная практика

3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Таблица 5

Вид учебной работы	Всего часов	Курс 4
Аудиторная контактная работа (всего), в том числе:	**10**	**10**
лекционные занятия (ЛЗ)	4	4
лабораторные работы (ЛР)	0	0
практические занятия (ПЗ)	6	6

Внеаудиторная контактная работа, КСР	**3**	**3**
Самостоятельная работа (всего), в том числе:	**91**	**91**
подготовка к устному опросу	31	31
самостоятельное изучение материала	30	31
подготовка к зачёту	30	30
Формы текущего контроля успеваемости	Вопросы к устному опросу	Вопросы к устному опросу
Формы промежуточной аттестации	**зачет**	**зачет**
Контроль	**4**	**4**
ИТОГО: час.	**108**	**108**
ИТОГО: з.е.	**3**	**3**

4. Содержание дисциплины, структурированное по темам (разделам), с указанием отведенного на них количества академических часов и видов учебных занятий

Таблица 6

№ раздела	Наименование раздела дисциплины	Виды учебной нагрузки и их трудоемкость, часы						
		ЛЗ	ЛР	ПЗ	СРС	КСР	Конт-роль	Всего часов
1	Методическое и техническое обеспечение ИБ функционирования предприятий	2	-	-	15	2	-	18
2	Основные понятия и определения предмета защиты информации	2	-	-	15	1	-	18
3	Разграничение доступа к ресурсам	-	-	2	15	-	1	18
4	Идентификация и аутентификация субъектов	-	-	-	16	-	1	18
5	Методы и средства криптографической защиты	-	-	2	15	-	1	18
6	Контроль целостности информации. Защита от РПВ	-	-	2	15	-	1	18
Итого:		**4**	**0**	**6**	**91**	**3**	**4**	**108**

4.1. Содержание лекционных занятий

Таблица 7

№ ЛЗ	Наименование раздела	Тема лекции	Содержание лекции (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Кол-во часов
Курс 4				
1	Методическое и техническое обеспечение ИБ функционирования предприятий	Комплексный и системный подход к обеспечению ИБ объектов, технических средств и физических лиц	Методология и содержание обеспечения ИБ при комплексном и системном подходе. Системная реализация защиты процессов переработки информации на отдельных объектах информационных систем управления. Общие вопросы организации противодействия информационной и технической агрессии. Защита технических средств и объектов предприятий от утечки информации и несанкционированного доступа.	2
2	Основные понятия и определения предмета защиты информации	Основные понятия и определения предмета защиты информации	Правовое обеспечение информационной безопасности. Организационно–распорядительная документация. Санкционированный и несанкционированный доступ. Субъект и объект доступа. Угрозы безопасности и каналы реализации угроз. Ключ, пароль, межсетевой экран.	2
Итого за курс:				**4**
Итого:				**4**

4.2. Содержание лабораторных занятий

Таблица 8

№ ЛР	Наименование раздела	Наименование лабораторной работы	Содержание лабораторной работы (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Кол-во часов
не предусмотрены учебным планом				

4.3. Содержание практических занятий

Таблица 9

№ ПЗ	Наименование раздела	Тема практического занятия	Содержание практического занятия (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Кол-во часов
Курс 4				

1	Разграничение доступа к ресурсам	Дискреционная политика безопасности. Разграничение доступа к ресурсам СУБД.	Создание дискреционной матрицы доступа. Контроль доступа, базирующийся на ролях. Разграничение доступа к ресурсам СУБД.	2
2	Методы и средства криптографической защиты	Помехоустойчивые коды. Построение кодов с обнаружением и исправлением ошибки.	Помехоустойчивые коды. Построение кодов с обнаружением и исправлением ошибки.	2
3	Контроль целостности информации. Защита от РПВ	Контроль целостности информации. Защита от РПВ.	Вычисления контрольной суммы.	2
			Итого за курс:	**6**
			Итого:	**6**

4.4. Содержание самостоятельной работы

Таблица 10

№ п/п	Наименование раздела	Вид самостоятельной работы	Содержание самостоятельной работы (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Кол-во часов
			Курс 4	
1	Разграничение доступа к ресурсам Методы и средства криптографической защиты Контроль целостности информации. Защита от РПВ	подготовка к устному опросу	Шифрование методом замены (подстановки): шифр Атбаш, шифр Цезаря, Шифры простой моноалфавитной замены, шифр Гронсфельда, шифр Вернама, Шифрование методами перестановки: Методы простой перестановки. Шифрование методом Гамильтона. Дешифрование методом замены (подстановки): шифр Атбаш, шифр Цезаря, Шифры простой моноалфавитной замены, Дешифрование методами перестановки: метод простой перестановки, метод Гамильтона. Алгоритм шифрования RSA. Контроль целостности информации Разграничение доступа к ресурсам СУБД	31
2	Все разделы	самостоятельное изучение материала	Дискреционные и мандатные политики безопасности. Уровни конфиденциальности объектов. Уровни допуска субъектов. Создание дискреционной матрицы доступа. Контроль доступа, базирующийся на ролях. Идентификация и аутентификация субъектов	30
3	Все разделы	подготовка к зачёту	Изучение тем, представленных в примерном перечне вопросов к зачету	30
			Итого за курс:	**91**
			Итого:	**91**

5. Методические указания для обучающихся по освоению дисциплины (модуля)

1. Методические указания при работе на лекции

До лекции студент должен просмотреть учебно-методическую и научную литературу по теме лекции для того, чтобы иметь представление о проблемах, которые будут подняты в лекции.

Перед началом лекции обучающимся сообщается тема лекции, план, вопросы, подлежащие рассмотрению, доводятся основные литературные источники. Весь учебный материал, сообщаемый преподавателем, должен не просто прослушиваться. Он должен быть активно воспринят, т. е. услышан, осмыслен, понят, зафиксирован на бумаге и закреплен в памяти. Приступая к слушанию нового учебного материала, полезно мысленно установить его связь с ранее изученным. Следя за техникой чтения лекции (акцент на существенном, повышение тона, изменение ритма, пауза и т. п.), необходимо вслед за преподавателем уметь выделять основные категории, законы и определять их содержание, проблемы, предполагать их возможные решения, доказательства и выводы. Осуществляя такую работу, можно значительно облегчить себе понимание учебного материала, его конспектирование и дальнейшее изучение.

2. Методические указания при подготовке и работе на практическом занятии

Практические занятия по дисциплине проводятся в целях выработки практических умений и приобретения навыков в решении профессиональных задач.

Подготовка обучающегося к практическому занятию производится по вопросам, разработанным для каждой темы практических занятий и (или) лекций. В процессе подготовки к практическим занятиям, необходимо обратить особое внимание на самостоятельное изучение рекомендованной литературы.

Работа студентов во время практического занятия осуществляется на основе заданий, которые выдаются обучающимся в начале или во время занятия. На практических занятиях приветствуется активное участие в обсуждении конкретных ситуаций, способность на основе полученных знаний находить наиболее эффективные решения поставленных проблем, уметь находить полезный дополнительный

материал по тематике занятий. На практических занятиях обучающиеся должны уметь выработать определенные решения по обозначенной проблеме. В зависимости от сложности предлагаемых заданий, целей занятия, общей подготовки обучающихся преподаватель может подсказать обучающимся алгоритм решения или первое действие, или указать общее направление рассуждений. Полученные результаты обсуждаются с позиций их адекватности или эффективности в рассмотренной ситуации.

3. Методические указания по подготовке к устному опросу

Самостоятельная работа обучающихся включает подготовку к устному опросу на семинарских занятиях. Для этого обучающийся изучает лекции, основную и дополнительную литературу, публикации, информацию из Интернет-ресурсов. Темы и вопросы к семинарским занятиям, вопросы для самоконтроля доводятся до обучающихся заранее. Эффективность подготовки обучающихся к устному опросу зависит от качества ознакомления с рекомендованной литературой. Для подготовки к устному опросу необходимо ознакомиться с материалом по теме семинар и обратить внимание на усвоение основных понятий изучаемой темы, выявить неясные вопросы и подобрать дополнительную литературу для их освещения, составить тезисы выступления по отдельным проблемным аспектам. В среднем, подготовка к устному опросу по одному семинарскому занятию занимает от 2 до 4 часов

4. Методические указания по самостоятельной работе

Организация самостоятельной работы обучающихся ориентируется на активные методы овладения знаниями, развитие творческих способностей, переход от поточного к индивидуализированному обучению с учетом потребностей и возможностей обучающегося.

Самостоятельная работа с учебниками, учебными пособиями, научной, справочной литературой, материалами периодических изданий и Интернета является наиболее эффективным методом получения дополнительных знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала. Все новые понятия по изучаемой теме необходимо выучить наизусть.

Самостоятельная работа реализуется:

- непосредственно в процессе аудиторных занятий;
- на лекциях, практических занятиях;
- в контакте с преподавателем вне рамок расписания;
- на консультациях по учебным вопросам, в ходе творческих контактов, при ликвидации задолженностей, при выполнении индивидуальных заданий и т. д.;
- в методическом кабинете, дома, на кафедре при выполнении обучающимся учебных и практических задач.

Эффективным средством осуществления обучающимся самостоятельной работы является электронная информационно-образовательная среда университета, которая обеспечивает доступ к учебным планам, рабочим программам дисциплин (модулей), практик, к изданиям электронных библиотечных систем.

6. Перечень учебной литературы и учебно-методического обеспечения для самостоятельной работы

Таблица 11

№ п/п	Автор(ы), наименование, место, год издания (если есть, указать «гриф»)	Книжный фонд (КФ) или электрон. ресурс (ЭР)	Литература	
			учебная	для самост. работы
1.	Информационная безопасность: учебно-методическое пособие / Фомин Д.В., Вузовское образование: 2018.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu||iprbooks||77320	ЭР	+	
2.	Методы и средства комплексной защиты информации в технических системах: учебное пособие / Запонов Э.В., Мартынов А.П., Машин И.Г., Николаев Д.Б., Сплюхин Д.В., Фомченко В.Н., Российский федеральный ядерный центр – ВНИИЭФ: 2019.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu||iprbooks||101925	ЭР	+	
3.	Методы и средства защиты информации: практикум / Бондаренко И.С., Демчишин Ю.В., Издательский Дом МИСиС: 2018.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu||iprbooks||84413	ЭР	+	
4.	Основы информационной безопасности: учебное пособие / Галатенко В.А., Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа: 2020.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu||iprbooks||97562	ЭР		+
5.	Информационная безопасность и защита информации: учебное пособие / Башлы П.Н., Бабаш А.В., Баранова Е.К., Евразийский открытый институт: 2012.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu||iprbooks||10677	ЭР		+
6.	Информационная безопасность и защита информации: учебник /	ЭР	+	

	Прохорова О.В., Самарский государственный архитектурно-строительный университет, ЭБС АСВ: 2014.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu||iprbooks||43183			
7.	Информационная безопасность и защита информации: учебное пособие / Шаньгин В.Ф., Профобразование: 2019.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu||iprbooks||87995	ЭР		+

Доступ обучающихся к ЭР НТБ СамГТУ (elib.samgtu.ru) осуществляется посредством электронной информационной образовательной среды университета и сайта НТБ СамГТУ по логину и паролю.

7. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

При проведении лекционных занятий используется мультимедийное оборудование. Организовано взаимодействие обучающегося и преподавателя с использованием электронной информационной образовательной среды университета.

Программное обеспечение

Таблица 12

№ п/п	Название	Способ распространения (лицензионное или свободно распространяемое)	Правообладатель (производитель)	Страна происхождения (иностранное или отечественное)
1.	Пакет офисных программ LibreOffice	свободно распространяемое	The Document Foundation	иностранное
2.	Пакет офисных программ Microsoft Office	лицензионное	Microsoft	иностранное
3.	Adobe Reader	свободно распространяемое	Adobe Systems Incorporated	иностранное
4.	Справочно-правовая система «Консультант Плюс»	лицензионное	НПО «ВМИ»	отечественное
5.	Антивирус Касперского	лицензионное	Лаборатория Касперского	отечественное
6.	Операционная система Microsoft Windows	лицензионное	Microsoft	иностранное
7.	Операционная система семейства Unix	свободно распространяемое	The Linux Foundation	иностранное
8.	Яндекс.Браузер	свободно распространяемое	Яндекс	отечественное

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», профессиональных баз данных, информационно-справочных систем

Таблица 13

№ п/п	Наименование	Краткое описание	Режим доступа
1	Электронно-библиотечная система IPRbooks	Электронно-библиотечная система	http://www.iprbookshop.ru/
2	Электронно-библиотечная система СамГТУ	Электронная библиотека СамГТУ	https://elib.samgtu.ru/
3	eLIBRARY.RU	Научная электронная библиотека	http://www.elibrary.ru/

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

Лекционные занятия

Аудитории для лекционных занятий укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории (наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук).

Практические занятия

Аудитории для практических занятий укомплектованы специализированной мебелью и техническими средствами обучения (проектор, экран, компьютер/ноутбук).

Самостоятельная работа

Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде СамГТУ:

методический кабинет (ауд. 9);

компьютерные классы (ауд. 6, 15).

10. Фонд оценочных средств по дисциплине

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации представлен в Приложении 1.

Полный комплект контрольных заданий или иных материалов, необходимых для оценивания результатов обучения по дисциплине, практике хранится на кафедре-разработчике в бумажном и электронном виде.

Приложение 1

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации

по дисциплине

Б1.В.03.13 «Безопасность информационных технологий и систем»

Код и направление подготовки (специальность)	**09.03.02 Информационные системы и технологии**
Направленность (профиль)	**Информационные системы и технологии**
Квалификация	**бакалавр**
Форма обучения	**заочная**
Год начала подготовки	**2023**
Выпускающая кафедра	**Инженерные технологии**
Кафедра-разработчик	**Инженерные технологии**
Объем дисциплины, ч. / з.е.	**108 / 3**
Форма контроля (промежуточная аттестация)	**зачет**

1. Перечень компетенций, индикаторов достижения компетенций и признаков проявления компетенций (дескрипторов), которыми должен овладеть обучающийся в ходе освоения образовательной программы

Универсальные компетенции

Таблица 1

Наименование категории (группы) компетенций	Код компетенции	Наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения
не предусмотрены учебным планом				

Общепрофессиональные компетенции

Таблица 2

Код компетенции	Наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения
не предусмотрены учебным планом			

Профессиональные компетенции

Таблица 3

Код компетенции	Наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения
ПК-1	Способность выполнять концептуальное, функциональное и логическое проектирование систем среднего и крупного масштаба и сложности	**ПК-1.4** Подготавливает методики оценки на соответствие требованиям и оценивает качества готовых информационных систем	**В4 ПК-1.4** Владеть: Способностью к сбору, обработке и анализу готовых систем на соответствие требованиям
		ПК-1.7 Обеспечивает безопасность и целостность данных информационных систем и технологий	**З8 ПК-1.7** Знать: Основные понятия и определения предмета защиты информации, методическое и техническое обеспечение информационной безопасности **У6 ПК-1.7** Уметь: Применять методы и средства криптографической защиты **В7 ПК-1.7** Владеть: Способами контроля целостности информации

Матрица соответствия оценочных средств запланированным результатам обучения

Таблица 4

Код и индикатор достижения компетенции	Оценочные средства						
	Раздел 1.	Раздел 2.	Раздел 3.	Раздел 4.	Раздел 5.	Раздел 6.	Промежуточная аттестация
	Методическое и техническое обеспечение ИБ функционирования предприятий	Основные понятия и определения предмета защиты информации	Разграничение доступа к ресурсам	Идентификация и аутентификация субъектов	Методы и средства криптографической защиты	Контроль целостности информации. Защита от РПВ	
	Вопросы к устному опросу						Зачет
ПК-1.4	В4 ПК-1.4	В4 ПК-1.4	В4 ПК-1.4	В4 ПК-1.4	В4 ПК-1.4	В4 ПК-1.4	В4 ПК-1.4
ПК-1.7	З8 ПК-1.7 У6 ПК-1.7 В7 ПК-1.7	З8 ПК-1.7 У6 ПК-1.7 В7 ПК-1.7	З8 ПК-1.7 У6 ПК-1.7 В7 ПК-1.7	З8 ПК-1.7 У6 ПК-1.7 В7 ПК-1.7	З8 ПК-1.7 У6 ПК-1.7 В7 ПК-1.7	З8 ПК-1.7 У6 ПК-1.7 В7 ПК-1.7	З8 ПК-1.7 У6 ПК-1.7 В7 ПК-1.7

2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций в ходе освоения образовательной программы

2.1. Формы текущего контроля успеваемости

Промежуточная аттестация проводится в виде письменного/устного опроса, тестирования и представляет собой ответы на 2 вопроса и выполнение тестовых заданий.

Примерный перечень вопросов для устного опроса

Номер задания	Правильный ответ	Содержание вопроса	Компетенция	Время выполнения задания, мин
1	Административный Политика информационной безопасности обычно представляет собой документ высокого уровня, в котором описывается общая стратегия безопасности организации. Обычно он создается руководителем организации и предназначен для обеспечения всестороннего понимания существующих мер безопасности. Уровень информационной безопасности, который обеспечивает политика, зависит от конкретных потребностей и требований организации.	К какому уровню обеспечения ИБ относится «Политика информационной безопасности», утвержденная руководителем в конкретной организации?	ПК-1	2
2	Конфиденциальность. Его часто используют для описания степени, в которой человек может сохранять конфиденциальность своей личной информации от других. В целом конфиденциальность — это право, которое люди имеют на свою личную информацию. Конфиденциальность часто используется для описания степени, в которой человек может сохранять конфиденциальность личной информации от других.	Дайте определение гарантии того, что конкретная информация доступна только тому кругу лиц, для кого она предназначена.	ПК-1	2
3	Аутентификация . Он используется для обеспечения того, чтобы только авторизованные пользователи могли получить доступ и использовать систему или приложение. Аутентификация может осуществляться с помощью различных методов, таких как пароли, токены и биометрическая идентификация.	Процесс проверки подлинности или подтверждения идентификации пользователя или системы	ПК-1	2
4	Тип атаки на компьютерную систему, при которой злоумышленники вводят в буфер больше данных, чем он может обработать или содержать	Что такое «атака переполнения буфера»?	ПК-1	2
5	Используется для защиты конфиденциальности, целостности и подлинности информации, передаваемой между клиентом (например, веб-браузером) и сервером.	Для чего используется защищенное соединение SSL/TLS?	ПК-1	2
6	Межсетевой экран (firewall) Межсетевой экран (МЭ, брандмауэр или Firewall) представляет собой программно-аппаратный или программный комплекс, который отслеживает сетевые пакеты, блокирует или разрешает их прохождение. В фильтрации трафика брандмауэр опирается на установленные параметры — чаще всего их называют правилами МЭ. Современные межсетевые экраны располагаются на периферии сети, ограничивают транзит трафика, установку нежелательных соединений и подобные действия за счет средств фильтрации и аутентификации.	Сетевое устройство или программное обеспечение, которое контролирует и фильтрует трафик между различными сетями, обеспечивая безопасность и защиту сети от несанкционированного доступа и атак – это …?	ПК-1	2
7	Программное обеспечение, которое используется для обнаружения, блокирования и удаления вредоносных программ, таких как вирусы, трояны, шпионское ПО и другие угрозы безопасности	Антивирус	ПК-1	2
8	Вирусы — это вредоносные программы, которые могут распространяться на другие компьютеры и сети. Фишинг — это тип атаки, при которой злоумышленник отправляет электронное письмо или текстовое сообщение, которое выглядит как полученное из законного источника, но на самом деле является фальшивой попыткой обманом заставить получателя раскрыть личную информацию. Сетевые атаки — это попытки получить несанкционированный доступ к сети или системе.	Вирусы, фишинг, сетевые атаки	ПК-1	2
9	Криптография — это процесс преобразования информации в секретный код для обеспечения ее безопасности. Аутентификация — это процесс проверки личности пользователя. Межсетевые экраны — это системы безопасности, которые предотвращают несанкционированный доступ к компьютерной	Криптография, аутентификация, межсетевые экраны и брандмауэры	ПК-1	2

	сети. Брандмауэры используются для защиты сетей от вредоносных действий, таких как взлом, вирусы и черви.			
10	Асимметричное шифрование — это криптографический метод, который позволяет двум разным сторонам безопасно обмениваться зашифрованными данными без необходимости совместного использования секретного ключа. Это означает, что одна сторона может зашифровать данные и отправить их другой стороне, а другая сторона может расшифровать данные, используя другой ключ. Это полезно для защиты конфиденциальных данных, таких как номера кредитных карт, пароли и другая конфиденциальная информация.	Асимметричное шифрование	ПК-1	2
11	SQL-инъекция — это тип атаки, которая происходит, когда злоумышленник внедряет вредоносный код SQL в базу данных, чтобы получить несанкционированный доступ к данным. Вредоносный код может использоваться для обхода механизмов аутентификации, изменения данных или даже удаления данных из базы данных.	SQL-инъекция	ПК-1	2
12	Атака заключается в попытке причинить вред, сделав недоступной целевую систему, например веб-сайт или приложение, для обычных конечных пользователей	В чем заключается отказ в обслуживании или (DoS) атака?	ПК-1	2
13	Ручной поиск, динамическое тестирование, статическое тестирование. Ручной поиск — это тип тестирования, при котором человек вручную ищет определенный элемент или функцию в приложении. Динамическое тестирование — это тип тестирования, при котором приложение тестируется в динамической среде, например в работающей системе. Статическое тестирование — это тип тестирования, при котором приложение тестируется в статической среде, например в тестовой лаборатории.	Какие методы обнаружения уязвимостей веб-приложений Вы знаете (назовите 3 примера)?	ПК-1	2

2.2. Формы промежуточной аттестации

Промежуточная аттестация проводится в виде письменного/устного опроса, тестирования и представляет собой ответы на 2 вопроса и выполнение тестовых заданий.

Примерный перечень вопросов для подготовки к зачету

Номер задания	Правильный ответ	Содержание вопроса	Компетенция	Время выполнения задания, мин
1	Криптографическая хеш-функция — это математический алгоритм, который принимает данные и выдает выходное значение фиксированного размера. Выходное значение — это уникальное представление входных данных, которое можно использовать для проверки их подлинности. Хэш-функции используются в криптографии для обеспечения целостности данных и предотвращения подделки данных.	21	ПК-1	2
2	Специализированное программное обеспечение, предназначенное для защиты компании от утечек информации	Что такое DLP (Data Loss Prevention)?	ПК-1	2
3	Инсайдеры — это лица, имеющие доступ к конфиденциальной или служебной информации, недоступной широкой публике. Прямое копирование — это копирование или загрузка конфиденциальной или служебной информации без разрешения.	Какие «прямые» каналы утечки информации Вы знаете?	ПК-1	2
4	Совокупность правил, процедур, практических методов и руководящих принципов в области ИБ, используемых организацией в своей деятельности. Политика информационной безопасности — это набор руководящих принципов и процедур, которые организация реализует для обеспечения безопасности своих информационных активов.	Политика безопасности информации	ПК-1	2

	Обычно это комбинация технических и нетехнических мер, предназначенных для защиты конфиденциальных данных от несанкционированного доступа, использования, раскрытия, изменения или уничтожения.			
5	Доступ к информации в нарушение должностных полномочий сотрудника, доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации.	Несанкционированный доступ к информации (НСД)	ПК-1	2
6	Способность пользователя скрывать свою личность и делать онлайн-действия без раскрытия своего настоящего имени, местонахождения или других персональных данных	Что такое анонимность?	ПК-1	2
7	Аппаратные средства, программные средства, административные средства Под аппаратным обеспечением понимаются физические компоненты компьютерной системы, такие как процессор, память и устройства хранения данных. Программное обеспечение — это программы и приложения, которые работают на оборудовании. Административные инструменты — это инструменты, используемые для управления и обслуживания аппаратного и программного обеспечения компьютерной системы. Примеры инструментов администрирования включают инструменты системного администрирования, антивирусное программное обеспечение и программное обеспечение для резервного копирования.	Какие методы можно использовать для защиты информации при передаче по сети?	ПК-1	2
8	Событие или ситуация, которая нарушает или угрожает безопасности информационной системы, компьютерных сетей или конфиденциальности данных.	Инцидент безопасности	ПК-1	2
9	Преступление, при котором злоумышленник несанкционированно использует личные данные и информацию о человеке, включая его имя, адрес, социальные страховые номера, банковские реквизиты и другую конфиденциальную информацию, с целью совершения мошенничества, финансовой выгоды или нанесения ущерба.	Кража личности (идентичности)	ПК-1	2
10	Риски утечки данных Риски утечки данных — это потенциальные риски, которые возникают в случае утечки конфиденциальных или конфиденциальных данных неавторизованным пользователям или системам. Это может привести к финансовому, юридическому или репутационному ущербу организации. Риски утечки данных могут быть вызваны злонамеренными или непреднамеренными действиями сотрудников, подрядчиков или других сторон.	Какие риски связаны с использованием открытых Wi-Fi сетей?	ПК-1	2
11	Защищенные протоколы передачи данных Протоколы безопасной передачи данных (SDTP) — это протоколы, используемые для безопасной передачи данных между двумя или более компьютерами. Они предназначены для обеспечения безопасной и безошибочной передачи данных. SDTP обычно используются в деловой и правительственной среде для передачи конфиденциальных и конфиденциальных данных. Некоторые распространенные SDTP включают протокол безопасной передачи файлов (SFTP), протокол безопасного копирования (SCP) и виртуальные частные сети (VPN).	К какой группе правил и алгоритмов, используемых для обеспечения безопасности, при передаче данных по сети, относятся технологии SSL/TLS, HTTPS и SSH?	ПК-1	2
12	Попытка причинить вред, сделав недоступной целевую систему, например веб-сайт или приложение, для обычных конечных пользователей. Обычно злоумышленники генерируют большое количество пакетов или запросов, которые в конечном счете перегружают работу целевой системы.	Атака «отказ в обслуживании»	ПК-1	2
13	Вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям.	Фишинг	ПК-1	2
14	Процесс исследования сетевых систем, приложений или устройств с целью обнаружения и выявления уязвимостей в их конфигурации, программном обеспечении или параметрах безопасности.	Сканирование уязвимостей	ПК-1	2
15	Метод оценки безопасности компьютерных систем или сетей средствами моделирования атаки злоумышленника	Пентестинг	ПК-1	2

16	Разновидность вредоносной программы, проникающая в компьютер под видом легитимного программного обеспечения, в отличие от вирусов и червей, которые распространяются самопроизвольно.	Троянская вирусная программа	ПК-1	2
17	Как называются угрозы со стороны внутренних сотрудников?	Инсайдерские угрозы	ПК-1	2
18	VPN- VPN (виртуальная частная сеть) — это услуга, которая позволяет вам подключаться к Интернету через безопасное зашифрованное соединение. Это означает, что ваши данные защищены от хакеров и других злоумышленников. VPN обычно используются людьми, которые работают из дома или теми, кому необходим доступ к конфиденциальным данным из удаленного места.	Какая технология позволяет обеспечивать одно или несколько сетевых соединений поверх другой сети?	ПК-1	2
19	Расширение HTTP, которое поддерживает шифрование и защищает данные пользователей при передаче в Интернете.	Протокол HTTPS	ПК-1	2
20	Особенность защиты мобильных устройств от вредоносного ПО заключается в том, что она требует многоуровневого подхода, включающего как программные, так и аппаратные меры безопасности. Сюда входит установка антивирусного программного обеспечения, использование надежных паролей, избежание подозрительных ссылок и загрузок, а также обновление вашего устройства последними обновлениями безопасности.	В чем заключается особенность защиты мобильных устройств от вредоносных программ?	ПК-1	2
21	2: публичный и приватный В криптографии открытый ключ — это математическая функция, которую можно использовать для шифрования данных, а закрытый ключ — это математическая функция, которую можно использовать для расшифровки данных. Открытый ключ доступен каждому, кто хочет зашифровать данные, а закрытый ключ доступен только владельцу.	Какое количество ключей используется при аутентификации посредством публичного ключа (PKI)? Назовите их.	ПК-1	2
22	Узел в компьютерной сети, который обеспечивает связь между различными сетями или сетевыми сегментами.	Межсетевой гейт	ПК-1	2
23	Тип кибератаки, при которой злоумышленник внедряется в коммуникационный канал между двумя пользователями или системами, притворяется одним из них и перехватывает, изменяет или подделывает передаваемые данные.	В чем заключается атака «человек посередине»?	ПК-1	2
24	Атаки отказа в обслуживании, атаки переполнения буфера, фишинг, вредоносное ПО, атаки перебора паролей и атаки на сетевую инфраструктуру	Какие основные типы атак на информационные системы существуют?	ПК-1	2
25	Сетевая точка доступа, созданная злоумышленником с целью обмана пользователей и перехвата их данных. Это недобросовестная Wi-Fi-сеть, которая имитирует легитимную точку доступа, но контролируется злоумышленником.	Что такое поддельная точка доступа Wi-Fi?	ПК-1	2
26	Биометрическая аутентификация Биометрическая аутентификация — это процесс проверки личности человека с использованием его уникальных физических или поведенческих характеристик. Это может включать в себя отпечатки пальцев, распознавание лиц, распознавание голоса и сканирование радужной оболочки глаза.	Какой вид аутентификации использует для проверки подлинности субъекта его физиологические или поведенческие характеристики?	ПК-1	2
27	1. Изолировать нарушение 2. Сообщить о нарушении 3. Собрать доказательства 4. Произвести анализ уязвимостей 5. Изменить пароли и учетные записи 6. Изолировать затронутые системы Провести расследование и анализ	Какие меры необходимо предпринять при обнаружении нарушений информационной безопасности?	ПК-1	2

Примерный перечень тестовых заданий к промежуточной аттестации

Номер задания	Правильный ответ	Содержание вопроса	Компетенция	Время выполнения задания, мин
1	Б	Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов и требований: а) защищенность информации б) защищаемая информация в) защищенность потребителей информации г) защита информации	ПК-1	2
2	Б	Согласование разнородных средств при построении целостной системы защиты, перекрывающий все существенные каналы реализации угроз и не содержащий слабых мест на стыках отдельных компонентов: а) принцип системности б) принцип комплексности в) принцип непрерывной защиты г) принцип разумной достаточности	ПК-1	2
3	Г	Гарантия того, что источником информации является именно то лицо, которое заявлено как ее автор: а) конфиденциальность б) целостность в) доступность г) аутентичность	ПК-1	2
4	А	Защищаемые государством сведения в области военной, внешнеполитической и внешнеэкономической деятельности, распространение которых может нанести ущерб безопасности РФ: а) государственная тайна б) коммерческая тайна в) банковская тайна г) конфиденциальная информация	ПК-1	2
5	В	К какому уровню доступа информации относится следующая информация: «Ложная реклама, реклама со скрытыми вставками…»: а) информация без ограничения права доступа б) информация с ограниченным доступом в) информация, распространение которой наносит вред интересам общества г) объект интеллектуальной собственности	ПК-1	2
6	В	Возможные воздействия на АС, которые прямо или косвенно могут нанести ущерб ее безопасности: а) комплексное обеспечение информационной безопасности б) безопасность АС в) угрозы информационной безопасности г) атака на автоматизированную систему	ПК-1	2
7	В	Непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла АС: а) принцип системности б) принцип комплексности в) принцип непрерывной защиты г) принцип разумной достаточности	ПК-1	2
8	Б	Свойство данных быть доступными для санкционированного пользования в произвольный момент времени, когда в обращении к ним возникает необходимость: а) конфиденциальность б) доступность в) аутентичность г) аппелируемость	ПК-1	2
9	А	Документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ: а) государственная тайна б) коммерческая тайна в) банковская тайна г) конфиденциальная информация	ПК-1	2
10	Г	Защита от случайных и преднамеренных воздействий, чреватых нанесением ущерба владельцам или пользователям информации это:	ПК-1	2

		а) защита информации б) компьютерная безопасность в) защищенность информации г) защищенность потребителей информации		
11	Г	К какому уровню доступа информации относится следующая информация: «Авторское право, патентное право…»: а) информация без ограничения права доступа б) информация с ограниченным доступом в) информация, распространение которой наносит вред интересам общества г) объект интеллектуальной собственности	ПК-1	2
12	Б	Информационно упорядоченная совокупность документов и информационных технологий, реализующая информационные процессы: а) информационные ресурсы б) информационная система в) информационная сфера г) информационные услуги	ПК-1	2
13	А	Набор аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных: а) защита информации б) компьютерная безопасность в) защищенность информации г) защищенность потребителей информации	ПК-1	2
14	А	К какому уровню доступа информации относится следующая информация: «Информация, содержащая сведения об обстоятельствах и фактах, предоставляющих угрозу жизни, здоровью граждан …»: а) информация без ограничения права доступа б) информация с ограниченным доступом в) информация, распространение которой наносит вред интересам общества г) объект интеллектуальной собственности	ПК-1	2
15	Г	Действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости системы: а) комплексное обеспечение информационной безопасности б) безопасность АС в) угроза информационной безопасности г) атака на автоматизированную систему	ПК-1	2
16	Г	Информация, не являющаяся общедоступной, которая ставит лиц, обладающих ею в силу своего служебного положения, в преимущественное положение по сравнению с другими объектами: а) служебная информация б) коммерческая тайна в) банковская тайна г) конфиденциальная информация	ПК-1	2
17	Б	Исследование возможности расшифрования информации без знания ключей: а) криптология б) криптоанализ в) взлом г) несанкционированный доступ	ПК-1	2
18	А	Идентификатор субъекта доступа, который является его секретом: а) пароль б) ключ в) электронно-цифровая подпись г) сертификат ключа подписи	ПК-1	2
19	Г	Деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения и несанкционированного доступа к защищаемой информации и от получения защищаемой информации: а) защита информации от непреднамеренного воздействия б) защита информации от несанкционированного воздействия в) защита информации от несанкционированного доступа г) защита от утечки информации	ПК-1	2
20	Б	Что не относится к информационной инфекции: а) троянский конь б) фальсификация данных в) черви г) вирусы	ПК-1	2
21	Г	Устройства, осуществляющие воздействие на человека путем передачи информации через внечувственное восприятие: а) средства массовой информации б) психотропные препараты в) психотронные генераторы г) средства специального программно-технического воздействия	ПК-1	2
22	А	Гарантия того, что конкретная информация доступна только тому кругу лиц, для кого она предназначена:	ПК-1	2

		а) конфиденциальность б) доступность в) аутентичность г) целостность		
23	Б	Информационная безопасность это: а) состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз б) состояние защищенности жизненно важных интересов личности, общества и государства в информационной сфере от внутренних и внешних угроз в) состояние, когда не угрожает опасность информационным системам г) политика национальной безопасности России	ПК-1	2
24	Б	К достоинствам технических средств защиты относятся: а) регулярный контроль б) создание комплексных систем защиты в) степень сложности устройства г) все варианты верны	ПК-1	2
25	В	Антивирусная программа принцип работы, которой основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых вирусов называется: а) ревизором б) иммунизатором в) сканером г) доктора и фаги	ПК-1	2
26	Г	Совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты АС от заданного множества угроз безопасности: а) комплексное обеспечение информационной безопасности б) безопасность АС в) угроза информационной безопасности г) политика безопасности	ПК-1	2
27	Г	Уровень защиты, при котором затраты, риск, размер возможного ущерба были бы приемлемыми: а) принцип системности б) принцип комплексности в) принцип непрерывности г) принцип разумной достаточности	ПК-1	2
28	Б	Информация, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличивать доходы, сохранить положение на рынке товаров, работ или услуг это: а) государственная тайна б) коммерческая тайна в) банковская тайна г) конфиденциальная информация	ПК-1	2
29	В	К вирусам, изменяющим среду обитания. относятся: а) черви б) студенческие в) полиморфные г) спутники	ПК-1	2
30	Б	Некоторое секретное количество информации, известное только пользователю и парольной системе, которое может быть запомнено пользователем и предъявлено для прохождения процедуры аутентификации это: а) идентификатор пользователя б) пароль пользователя в) учетная запись пользователя г) парольная система	ПК-1	2
31	Г	К видам системы обнаружения атак относятся: а) системы, обнаружения атаки на ОС б) системы, обнаружения атаки на конкретные приложения в) системы, обнаружения атаки на удаленных БД г) все варианты верны	ПК-1	2
32	Б	Вирусы, не связывающие свои копии с файлами, а создающие свои копии на дисках, не изменяя других файлов, называются: а) компаньон - вирусами б) черви в) паразитические г) стелс - вирусы	ПК-1	2
33	Б	К какому уровню обеспечения ИБ относится «Политика информационной безопасности», утвержденная руководителем в конкретной организации? а) законодательный б) административный в) процедурный г) научно-технический	ПК-1	2
34	Б	Кто такой инсайдер?	ПК-1	2

		а) внешний злоумышленник б) внутренний злоумышленник в) человек, разработавший вредоносную программу г) человек, подвергшийся атаке злоумышленника		
35	В	Как называется практически бесполезная информация, рассылаемая абонентам электронной почты? а) DoS б) virus в) spam г) worm	ПК-1	2

3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций

3.1. Характеристика процедуры текущей и промежуточной аттестации по дисциплине

Таблица 5

№ п/п	Наименование оценочного средства	Периодичность и способ проведения процедуры оценивания	Методы оценивания	Виды выставляемых оценок	Способ учета индивидуальных достижений, обучающихся
1.	Вопросы к устному опросу	систематически на практических занятиях / письменно и устно	экспертный	По пятибалльной шкале	рабочая книжка преподавателя
2.	Промежуточная аттестация – вопросы к зачету	по окончании изучения дисциплины/ устно и письменно	экспертный	Зачет/незачет	зачетная ведомость, зачетная книжка

3.2. Критерии и шкала оценивания результатов изучения дисциплины во время занятий (текущий контроль успеваемости)

Критерии оценки и шкала оценивания вопросов к устному опросу

Таблица 6

Шкала оценивания	Критерии оценки	Кол-во баллов
«Отлично»	Студент показывает полные и глубокие знания программного материала, логично и аргументировано отвечает на поставленный вопрос, а также дополнительные вопросы, показатели рейтинга (все предусмотренные РПД учебные задания выполнены, качество выполнения большинства из них оценено числом баллов, близким к максимальному).	46-100 баллов
«Хорошо»	Студент показывает глубокие знания программного материала, грамотно его излагает, достаточно полно отвечает на поставленный вопрос и дополнительные вопросы, умело формулирует выводы, допуская незначительные погрешности, показатели рейтинга (все предусмотренные РПД учебные задания выполнены, качество выполнения ни одного из них не оценено максимальным числом баллов).	26-45 баллов
«Удовлетворительно»	Студент показывает достаточные, но неглубокие знания программного материала; при ответе не допускает грубых ошибок или противоречий, однако в формулировании ответа отсутствует должная связь между анализом, аргументацией и выводами, для получения правильного ответа требуется уточняющие вопросы, достигнуты минимальные или выше показатели рейтинговой оценки при наличии выполнения предусмотренных РПД учебных заданий	5-25 баллов
«Неудовлетворительно»	Ответы на вопросы даны не верно	0 баллов

Общие критерии и шкала оценивания результатов для допуска к промежуточной аттестации

Таблица 7

Наименование оценочного средства		Балльная шкала
1.	Вопросы к устному опросу	0-100 баллов
	Итого:	100 баллов

Максимальное количество баллов за семестр – 100. Обучающийся допускается к зачету при условии 51 и более набранных за семестр баллов.

3.3 Критерии и шкала оценивания результатов изучения дисциплины на промежуточной аттестации

Основанием для определения оценки на зачете служит уровень освоения обучающимися материала и формирования компетенций, предусмотренных программой учебной дисциплины.

Успеваемость на зачете определяется оценками: «зачтено», «не зачтено».

Оценку «зачтено» получает обучающийся, освоивший компетенции дисциплины на всех этапах их формирования на 51-100 %, показавший всестороннее, систематическое и глубокое знание учебного

материала, умение свободно выполнять задания, предусмотренные рабочей программой, усвоивший основную и ознакомленный с дополнительной литературой, рекомендованной программой. Как правило, оценка «зачтено» выставляется обучающимся, усвоившим взаимосвязь основных положений учебной дисциплины, необходимых для приобретаемой профессии, проявившим творческие способности в понимании, изложении и использовании учебного материала.

Оценка «не зачтено» выставляется обучающемуся, освоившему компетенции дисциплины на всех этапах их формирования менее чем на 51%, обнаружившему пробелы в знаниях основного учебного материала, допустившему принципиальные ошибки в выполнении предусмотренных рабочей программой заданий.

Шкала оценивания результатов

Таблица 8

Процентная шкала (при ее использовании)	**Оценка в системе «неудовлетворительно – удовлетворительно – хорошо – отлично»**
0-50%	Не зачтено
51-100%	Зачтено

Приложение 2

УТВЕРЖДАЮ
Директор филиала ФГБОУ ВО «СамГТУ»
в г. Белебее Республики Башкортостан

_____ Л.М. Инаходова
«____» _____ 20__ г.

Дополнения и изменения к рабочей программе дисциплины (модуля)

Б1.В.03.13 «Безопасность информационных технологий и систем»

по направлению подготовки (специальности) 09.03.02 «Информационные системы и технологии» по направленности (профилю) подготовки «Информационные системы и технологии»

на 20__/20__ учебный год

В рабочую программу вносятся следующие изменения:

1) .....;
2) .....;

Разработчик дополнений и изменений:

_____	_____	_____
(должность, степень, ученое звание)	(подпись)	(ФИО)

Дополнения и изменения рассмотрены и одобрены на заседании кафедры «____» _____ 20___ г., протокол № ____.

Заведующий кафедрой

_____	_____
(степень, звание, подпись)	(ФИО)

Приложение 3

Аннотация рабочей программы дисциплины

Б1.В.03.13 «Безопасность информационных технологий и систем»

Код и направление подготовки (специальность) **09.03.02 Информационные системы и технологии**

Направленность (профиль) **Информационные системы и технологии**

Квалификация **бакалавр**

Форма обучения **заочная**

Год начала подготовки **2023**

Выпускающая кафедра **Инженерные технологии**

Кафедра-разработчик **Инженерные технологии**

Объем дисциплины, ч. / з.е. **108 / 3**

Форма контроля (промежуточная аттестация) **зачет**

Курс	Час. / з.е.	Лек. зан., час.	Лаб. зан., час.	Практич. зан., час.	КСР	СРС	Контроль	Форма контроля
7	108 / 3	4	-	6	3	91	4	зачет
Итого	108 / 3	4	-	6	3	91	4	зачет

Универсальные компетенции:	
не предусмотрены учебным планом	
Общепрофессиональные компетенции:	
не предусмотрены учебным планом	
Профессиональные компетенции:	
ПК-1	Способность выполнять концептуальное, функциональное и логическое проектирование систем среднего и крупного масштаба и сложности
ПК-1.4	Подготавливает методики оценки на соответствие требованиям и оценивает качества готовых информационных систем
ПК-1.7	Обеспечивает безопасность и целостность данных информационных систем и технологий

Содержание дисциплины охватывает круг вопросов, связанных с концептуальными основами обеспечения информационной безопасности автоматизированных и информационных систем, подходами к анализу и оценке рисков информационной безопасности, а также связанных с оценкой уровня защищенности автоматизированных и информационных систем.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, практические занятия, самостоятельная работа студента.

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости в форме вопросов к устному опросу и промежуточный контроль в форме: зачет.