Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Кубанский государственный университет»
Факультет компьютерных технологий и прикладной математики

«30» мая 2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.04 Информационная безопасность в облачных средах

Направление подготовки 01.04.02 Прикладная математика и информатика

Направленность (профиль) Математическое моделирование в естествознании и технологиях

Форма обучения очная

Квалификация магистр

Краснодар 2025

Рабочая программа дисциплины «Математическое моделирование в технике и технологиях» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 01.04.02 Прикладная математика и информатика

Программу составил:

Тыщенко В.В., ведуший разработчик АО «Точка»
Прутский А.С., преподаватель кафедры информационных технологий КубГУ

Рабочая программа дисциплины «Информационная безопасность в облачных средах» утверждена на заседании кафедры математического моделирования протокол №11 от «22» мая 2025 г.

Заведующий кафедрой (разработчика) акад. РАН,
д-р физ.-мат. наук, проф. Бабешко В.А. _____
подпись

Утверждена на заседании учебно-методической комиссии факультета компьютерных технологий и прикладной математики
протокол №4 от «23» мая 2025 г.
Председатель УМК факультета
д-р. техн. наук, доцент Коваленко А.В. _____
подпись

Рецензенты:

Калинчук В.В., д-р физ.-мат. наук, заведующий отделом математики, механики и нанотехнологий Южного научного центра РАН

Халафян А.А., д-р техн. наук, профессор кафедры анализа данных и искусственного интеллекта КубГУ

1 Цели и задачи изучения дисциплины

1.1 Цель освоения дисциплины

Цели изучения дисциплины определены государственным образовательным стандартом высшего образования. Цели изучения дисциплины соотнесены с общими целями ООП ВО по направлению подготовки «Прикладная математика и информатика», в рамках которой преподается дисциплина.

Данная дисциплина ставит своей **целью** изучение истории появления информационной безопасности, отечественных и зарубежных регламентов, получение опыта эффективного использования принципов информационной безопасности в облачных средах, формирование профессиональных навыков управление доступом.

Процесс освоения данной дисциплины направлен на получения необходимого объема теоретических знаний, отвечающих требованиям ФГОС ВО и обеспечивающих успешное проведение магистром профессиональной деятельности, владение методологией формулирования и решения прикладных задач, а также на выработку умений применять на практике принципы информационной безопасности. Цели дисциплины соответствуют следующим формируемым компетенциям: ПК-1, ПК-2, ПК-5.

1.2 Задачи дисциплины

Основные **задачи** дисциплины:

- идентификация угроз безопасности облачной информационной системы, а также обзор основных методов защиты информации в облачных системах;
- формирование навыков оценки возможных угроз безопасности в облачной системе;
- формирование навыков использования основных средств защиты информации в облачных технологиях.

1.3 Место дисциплины в структуре образовательной программы.

Дисциплина «Информационная безопасность в облачных средах» относится к вариативной части Блока 1 «Дисциплины (модули)» учебного плана программы подготовки магистров, базируется на знаниях, полученных по стандарту высшего образования, и является необходимой для теоретической подготовки магистров по программе «Математическое моделирование в естествознании и технологиях».

Место курса в профессиональной подготовке магистра определяется ролью навыков информационной безопасности в формировании высококвалифицированного специалиста в любой области знаний, использующей информационные системы и технологии. Данная дисциплина является важным звеном в обеспечении магистра знаниями, позволяющими успешно вести профессиональную деятельность. Имеется логическая и содержательно-методическая взаимосвязь с другими частями ООП ВО. Дисциплина «Информационная безопасность в облачных средах» связана с дисциплинами базового цикла и другими дисциплинами вариативной части. Данный курс наиболее тесно связан с курсами «Технологии проектирования и сопровождения программных систем» и «Современные проблемы прикладной математики и информатики».

Необходимым требованием к «входным» знаниям, умениям и опыту обучающегося при освоении данной дисциплины, приобретенным в результате освоения предшествующих дисциплин является уверенное владения материалом следующих курсов: Основы информационной безопасности, Методы программирования, Разработка приложений в интегрированных средах, Технологии программирования.

1.4 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы.

В результате освоения курса «Информационная безопасность в облачных средах» обучающийся должен обладать профессиональными компетенциями:

ПК-1 **Способен формулировать и решать актуальные и значимые задачи фундаментальной и прикладной математики**

Знать ИПК-1.1 (D/29.7 Зн.8) Современный отечественный и зарубежный опыт в решении актуальных и значимых задач фундаментальной и прикладной математики

ИПК-1.2 (A/01.6 Зн.1) Методы и приемы формализации задач фундаментальной и прикладной математики

Уметь ИПК-1.3 (D/01.6 У.1) Проводить анализ исполнения требований при решении задач фундаментальной и прикладной математики

ИПК-1.4 (A/01.6 У.1) Использовать методы и приемы формализации актуальных и значимых задач фундаментальной и прикладной математики

ИПК-1.5 (D/04.7 У.1) Планировать проектные работы, формулировать и решать актуальные и значимые задачи фундаментальной и прикладной математики

Владеть ИПК-1.7 (D/04.7 Тд.4) Распределение ролей и аналитических работ по участникам аналитической группы проекта при решении задач фундаментальной и прикладной математики

ИПК-1.8 (D/04.7 Тд.5) Ответы на вопросы и предложения участников аналитической группы проекта при решении задач фундаментальной и прикладной математики

ПК-2 **Способен эффективно планировать необходимые ресурсы и этапы выполнения работ в области математического моделирования и информационно-коммуникационных технологий, составлять на высоком уровне соответствующие технические описания и инструкции**

Знать ИПК-2.1 (D/01.6 Зн.2) Возможности современных и перспективных средств разработки программных продуктов, технических средств в области математического моделирования и информационно-коммуникационных технологий

ИПК-2.2 (D/01.6 Зн.3) Методологии разработки программного обеспечения и технологии программирования, методы планирования и этапы выполнения работ в области математического моделирования и информационно-коммуникационных технологий

Уметь ИПК-2.8 (D/01.6 У.1) Проводить анализ исполнения требований, эффективно планировать необходимые ресурсы и этапы выполнения работ в области математического моделирования и информационно-коммуникационных технологий, составлять на высоком уровне соответствующие технические описания и инструкции

ИПК-2.11 (D/29.7 У.2) Разрабатывать регламентные документы, составлять на высоком уровне соответствующие технические описания и инструкции

Владеть ИПК-2.18 (D/01.6 Тд.4) Оценка и согласование сроков выполнения поставленных задач, планирование необходимых ресурсов и этапов выполнения работ в области математического моделирования и информационно-коммуникационных технологий, составление на высоком уровне соответствующих технических описаний и инструкциий

ПК-5 **Способен составлять и публично представлять научные обзоры, рефераты и отчеты по тематике проводимых исследований, а также подготовить научную публикацию**

Уметь ИПК-5.7 (A/01.6 У.8) Применять лучшие мировые практики оформления программного кода, составлять и публично представлять отчеты по тематике проводимых исследований

Владеть ИПК-5.12 (D/04.7 Тд.5) Ответы на вопросы и предложения участников аналитической группы проекта, представление соответствующих обзоров и документов

Результаты обучения по дисциплине достигаются в рамках осуществления всех видов контактной и самостоятельной работы обучающихся в соответствии с утвержденным учебным планом.

ПК-1	Способен находить и извлекать актуальную научно-техническую информацию из электронных библиотек, реферативных журналов и т.п.	
ИПК-1.1 (D/29.7 Зн.8) Современный отечественный и зарубежный опыт в решении актуальных и значимых задач фундаментальной и прикладной математики ИПК-1.2 (A/01.6 Зн.1) Методы и приемы формализации задач фундаментальной и прикладной математики ИПК-1.3 (D/01.6 У.1) Проводить анализ исполнения требований при решении задач фундаментальной и прикладной математики ИПК-1.4 (A/01.6 У.1) Использовать методы и приемы формализации актуальных и значимых задач фундаментальной и прикладной математики ИПК-1.3 (D/01.6 У.1) Проводить анализ исполнения требований при решении задач фундаментальной и прикладной математики ИПК-1.4 (A/01.6 У.1) Использовать методы и приемы формализации актуальных и значимых задач фундаментальной и прикладной математики ИПК-1.5 (D/04.7 У.1) Планировать проектные работы, формулировать и решать актуальные и значимые задачи фундаментальной и прикладной математики ИПК-1.7 (D/04.7 Тд.4) Распределение ролей и аналитических работ по участникам аналитической группы проекта при решении задач фундаментальной и прикладной математики ИПК-1.8 (D/04.7 Тд.5) Ответы на вопросы и предложения участников аналитической группы проекта при решении задач	**Знает**	современные методы анализа сетевых уязвимостей, методы и подходы к поиску и устранению уязвимостей. Методы и приемы формализации задач сетевой, серверной, программной безопасности.
	Умеет	планировать анализ исполнения требований программной безопасности в рамках установленной нормативной базы предприятия.
	Владеет	методами и приемами формализации актуальных сетевых и программных уязвимостей для программных продуктов в облачных средах.

фундаментальной и прикладной математики		
ПК-2	Способен эффективно планировать необходимые ресурсы и этапы выполнения работ в области математического моделирования и информационно-коммуникационных технологий, составлять на высоком уровне соответствующие технические описания и инструкции	
ИПК-2.1 (D/01.6 Зн.2) Возможности современных и перспективных средств разработки программных продуктов, технических средств в области математического моделирования и информационно-коммуникационных технологий ИПК-2.2 (D/01.6 Зн.3) Методологии разработки программного обеспечения и технологии программирования, методы планирования и этапы выполнения работ в области математического моделирования и информационно-коммуникационных технологий ИПК-2.8 (D/01.6 У.1) Проводить анализ исполнения требований, эффективно планировать необходимые ресурсы и этапы выполнения работ в области математического моделирования и информационно-коммуникационных технологий, составлять на высоком уровне соответствующие технические описания и инструкции ИПК-2.11 (D/29.7 У.2) Разрабатывать регламентные документы, составлять на высоком уровне соответствующие технические описания и инструкции ИПК-2.18 (D/01.6 Тд.4) Оценка и согласование сроков выполнения поставленных задач, планирование необходимых ресурсов и этапов выполнения работ в области математического моделирования и информационно-коммуникационных технологий, составление на высоком уровне соответствующих технических описаний и инструкций	**Знает**	возможности современных и перспективных средств в области поиска и анализа сетевых, программных, серверных уязвимостей в рамках разработки программного обеспечения. методологии разработки программного обеспечения и технологии программирования, методы планирования и этапы выполнения работ
	Умеет	проводить анализ исполнения требований сетевой и программной безопасности, учитывая современные описания CVE, оформляя отчеты по выявленным уязвимостям. составлять технические описания и инструкции по результатам выявления уязвимостей.
	Владеет	правилами разработки регламентационной документации для решения задач по предотвращению программных уязвимостей разрабатываемого программного обеспечения.
ПК-5	Способен составлять и публично представлять научные обзоры, рефераты и отчеты по тематике проводимых исследований, а также подготовить научную публикацию	
ИПК-5.7 (A/01.6 У.8) Применять лучшие мировые практики оформления программного кода, составлять и публично представлять отчеты по тематике проводимых исследований ИПК-5.12 (D/04.7 Тд.5) Ответы на вопросы и предложения	**Умеет**	применять лучшие мировые практики оформления программного кода для улучшения прозрачности и сетевой безопасности разрабатываемого продукта.
	Владеет	умением составления документации к программному продукту, позволяющего улучшить качество разработки программного продукта и увеличить уровень безопасности разрабатываемого ПО.

участников аналитической группы проекта, представление соответствующих обзоров и документов		

Процесс освоения дисциплины «Информационная безопасность в облачных средах» направлен на получения необходимого объема теоретических знаний и практических навыков, отвечающих требованиям ФГОС ВО и обеспечивающих успешное ведение магистром профессиональной деятельности.

2. Структура и содержание дисциплины

2.1 Распределение трудоёмкости дисциплины по видам работ

Общая трудоёмкость дисциплины составляет 3 зачетных единицы, 108 академических часов (из них 28 аудиторных). Курс «Информационная безопасность в облачных средах» состоит из лекционных и лабораторных занятий, сопровождаемых регулярной индивидуальной работой преподавателя со студентами в процессе самостоятельной работы. В конце семестра проводится экзамен. Программой дисциплины предусмотрены 14 часов лекционных и 14 часов лабораторных занятий.

Вид учебной работы		Всего часов	Семестр (часы)
			3
Контактная работа (всего)		**28,2**	**28,2**
В том числе:			
Занятия лекционного типа		14	14
Занятия семинарского типа (семинары, практические занятия)		–	–
Лабораторные занятия		14	14
Иная контактная работа:			
Контроль самостоятельной работы (КСР)		–	–
Промежуточная аттестация (ИКР)		0,3	0,3
Самостоятельная работа (всего)		**44**	**44**
В том числе:			
Курсовая работа		–	–
Проработка учебного (теоретического) материала		57	57
Подготовка к текущему контролю		21,8	21,8
Контроль: экзамен			
Подготовка к экзамену		**35,7**	**35,7**
Общая трудоемкость	**час.**	**108**	**108**
	в том числе контактная работа	**28,3**	**28,3**
	зач. ед	**3**	**3**

2.2 Структура дисциплины

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы (темы) дисциплины, изучаемые в 3 семестре

№	Наименование разделов	Количество часов			
		Всего	Аудиторная работа		Внеаудиторная работа
			Л	ЛЗ	СРС
1	2	3	4	5	7
1.	Введение в информационную безопасность	1	1	–	–
2.	Применение асимметричного шифрования.	9	3	2	4
3.	Безопасность контейнеров.	6	1	1	4
4.	Мониторинг, аудит, выявление аномалий и реагирование на инциденты в облачных средах.	6	1	1	4
5.	WAF, DDoS	6	1	1	4
6.	ИИ и социальная инженерия	7	1	–	6
7.	Правовые аспекты.	4	1	1	2
8	Популярные веб-уязвимости (языков программирования)	5	1	2	2
9	Популярные веб-уязвимости (инфраструктуры)	7	1	2	4
10	Популярные веб-уязвимости (фронтенд)	7	1	2	4
11	Аутентификация и управление доступом: многофакторная аутентификация и IAM + OAuth/OIDC	9	1	2	6
12	Беспроводные сети	5	1	–	4
Промежуточная аттестация (ИКР)		0,3	–	–	–
Подготовка к экзамену		35,7			
Итого:		**108**	**14**	**14**	**44**

Примечание: Л – лекции, ЛР – лабораторные занятия, СРС – самостоятельная работа студента.

2.3 Содержание разделов (тем) дисциплины

2.3.1 Занятия лекционного типа

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
1.	Введение в информационную безопасность.	История появления информационной безопасности. Регламенты GDPR, PCI DSS, HIPAA, отечественные. Громкие прецеденты и последствия.	–
2.	Применение асимметричного шифрования.	Центры сертификации, различия ECDSA/RSA, TLS 1.2/1.3, подписи драйверов, letsencrypt. Постквантовая криптография.	Опрос по результатам индивидуального задания

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
3.	Безопасность контейнеров.	Система контейнеризации. Утилиты для проверки и анализа слоёв контейнер. Анализ методов нарушения безопасности изоляции контейнера (побег из песочницы)	Опрос
4.	Мониторинг, аудит, выявление аномалий и реагирование на инциденты в облачных средах.	Система оркестрации контейнеров. Утилиты для выявления аномалий, политики сетевых доступов в k8s.	Опрос
5.	WAF, DDoS	Принципы работы сетевой безопасности. Web application firewall, защита от DDoS.	Опрос по результатам индивидуального задания;
6.	ИИ и социальная инженерия	Методы нарушения приватности в сети на примере дипфейков. Социальная инженерия, личная информационная безопасность.	Подготовка (защита) группового задания
7.	Правовые аспекты.	Уголовный кодекс РФ в рамках сетевой безопасности. Базы данных уязвимостей и дефектов безопасности на примере CVE. Разделение ролей в рамках сетевой безопасности (blue team, red team). Программы поиска уязвимостей (bug bounty), платформы для тренировки..	Подготовка презентации, Защита группового задания
8.	Популярные веб-уязвимости (языков программирования)	Популярные уязвимости по классам. Удаленное выполнение кода (RCE), неправомерный доступ к данным(SQLi, noSQLi), исполнение внешних данных xml(XXE)	Опрос по результатам индивидуального задания
9.	Популярные веб-уязвимости (инфраструктуры)	Нарушение маршрутизации (trailing slash), уязвимости в области контроля доступа веб приложений (IDOR)	Опрос
10.	Популярные веб-уязвимости (фронтенд)	Выполнение нежелательных действий в веб приложении (CSRF), выполнение вредоносного скрипта (XSS), доступ к внешним ресурсам (CORS).	Опрос
11.	Аутентификация и управление доступом: многофакторная аутентификация и IAM + OAuth/OIDC	Разбор работы OAuth и OIDC, стандарты авторизации.	Опрос по результатам индивидуального задания
12.	Беспроводные сети	Атаки на bluetooth и WiFi. Передача данных в недоверенных средах.	Опрос

2.3.2 Занятия семинарского типа

Учебный план не предусматривает занятий семинарского типа по дисциплине «Информационная безопасность в облачных средах»

2.3.3 Лабораторные занятия

№	Наименование лабораторных работ	Форма текущего контроля
1	3	4
1	Ознакомление с системами сертификатов подлинности веб-сайта, обеспечивающего безопасное соединение. Выпуск сертификата letsencrypt и проверка работоспособности.	Отчет по ЛР
2	Знакомство с универсальными сканерами безопасности на примере trivy. Методы проверки образов контейнеров в открытом доступе на примере docker hub. Написание эвристик.	Отчет по ЛР
3	Реализация защиты от сетевых распределенных атак (DDoS) с использованием языка lua и веб сервера nginx. Решение базовых задач на веб серверах.	Отчет по ЛР
4	Решение практических задач по системам безопасности на учебных серверах. Программные уязвимости SQLi, XSS.	Отчет по ЛР
5	Решение практических задач по системам безопасности на учебных серверах. Уязвимости инфраструктуры (trailing slash, IDOR)	Отчет по ЛР
6	Решение практических задач по системам безопасности на учебных серверах. Веб уязвимости (CORS, XSS)	Отчет по ЛР
7.	Диаграмма последовательностей для OAuth/OIDC. Анализ безопасности и возможные угрозы.	Отчет по ЛР

2.3.4 Примерная тематика курсовых работ

Учебный план не предусматривает занятий курсовых работ по дисциплине «Информационная безопасность в облачных средах».

2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
1	Подготовка к текущему контролю, подготовка индивидуальных зада–ний	1. Методические указания по организации и выполнению самостоятельной работы, утвержденные на заседании кафедры математического моделирования факультета компьютерных технологий и прикладной математики ФГБОУ ВО «КубГУ», протокол № 10 от 30.03.2018

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

2.5 Самостоятельное изучение разделов дисциплины

Целью самостоятельной работы является углубление знаний, полученных в результате аудиторных занятий. Содержание приведенной основной и дополнительной литературы позволяет охватить обширный круг задач и методов сейсмологии и механики деформируемого твердого тела.

3. Образовательные технологии

Программа по дисциплине предусматривает использование в учебном процессе следующих образовательные технологии: чтение лекций с использованием мультимедийных технологий; работа над индивидуальными заданиями с использованием пакетов прикладных программ, разбор конкретных ситуаций на практических занятиях.

Компьютерные технологии предоставляют средства разнопланового отображения алгоритмов и демонстрационного материала.

Подход разбора конкретных ситуаций широко используется как преподавателем, так и бакалаврами во время лекций и анализа результатов самостоятельной работы. Это обусловлено тем, что в процессе моделирования часто встречаются задачи, для которых единых подходов не существует. При исследовании и решении каждой конкретной задачи имеется, как правило, несколько методов, а это требует разбора и оценки целой совокупности конкретных ситуаций.

При обучении используются следующие образовательные технологии:

– Технология коммуникативного обучения – направлена на формирование коммуникативной компетентности студентов, которая является базовой, необходимой для адаптации к современным условиям межкультурной коммуникации.

– Технология разноуровневого (дифференцированного) обучения – предполагает осуществление познавательной деятельности студентов с учётом их индивидуальных способностей, возможностей и интересов, поощряя их реализовывать свой творческий потенциал.

– Технология модульного обучения – предусматривает деление содержания дисциплины на достаточно автономные разделы (модули), интегрированные в общий курс.

– Информационно-коммуникационные технологии (ИКТ) - расширяют рамки образовательного процесса, повышая его практическую направленность, способствуют интенсификации самостоятельной работы учащихся и повышению познавательной активности.

– Интернет-технологии – предоставляют широкие возможности для поиска информации, разработки научных проектов, ведения научных исследований.

– Технология индивидуализации обучения – помогает реализовывать личностно-ориентированный подход, учитывая индивидуальные особенности и потребности учащихся.

– Проектная технология – ориентирована на моделирование социального взаимодействия учащихся с целью решения задачи, которая определяется в рамках профессиональной подготовки, выделяя ту или иную предметную область.

– Технология обучения в сотрудничестве – реализует идею взаимного обучения, осуществляя как индивидуальную, так и коллективную ответственность за решение учебных задач.

– Технология развития критического мышления – способствует формированию разносторонней личности, способной критически относиться к информации, умению отбирать информацию для решения поставленной задачи.

Комплексное использование в учебном процессе всех вышеназванных технологий стимулируют личностную, интеллектуальную активность, развивают познавательные процессы, способствуют формированию компетенций, которыми должен обладать будущий специалист.

Семестр	Вид занятия	Используемые интерактивные образовательные технологии	Общее количество часов
3	Л	Интерактивная подача материала с мультимедийной системой. Обсуждение сложных и дискуссионных вопросов.	14
	ЛР	Компьютерные занятия в режимах взаимодействия «преподаватель – студент» и «студент – студент»	14
Итого:			28

Цель ***лекции*** – предоставление структурированной теоретической базы материала курса. Основные понятия и примеры применения.

Цель ***лабораторного занятия*** – научить применять теоретические знания при решении и исследовании конкретных задач. Лабораторные занятия проводятся в компьютерных классах, при этом практикуется работа в группах.

Групповые индивидуальные задания формируют навыки исследовательской работы в коллективе.

Внеаудиторные формы работы: написание реферата; работа с литературой и электронными ресурсами.

Темы, задания и вопросы для самостоятельной работы призваны сформировать навыки поиска информации, умения самостоятельно расширять и углублять знания, полученные в ходе лекционных и лабораторных занятий.

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

4 Оценочные и методические материалы

4.1 Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

Учебная деятельность проходит в соответствии с графиком учебного процесса. Процесс самостоятельной работы контролируется во время аудиторных занятий и индивидуальных консультаций. Самостоятельная работа студентов проводится в форме изучения отдельных теоретических вопросов по предлагаемой литературе.

Фонд оценочных средств дисциплины состоит из средств текущего контроля (см. список лабораторных работ, задач и вопросов) и итоговой аттестации (зачета).

В качестве оценочных средств, используемых для текущего контроля успеваемости, предлагается перечень вопросов, которые прорабатываются в процессе освоения курса. Данный перечень охватывает все основные разделы курса, включая знания, получаемые во время самостоятельной работы. Кроме того, важным элементом технологии является самостоятельное решение студентами и сдача заданий. Это полностью индивидуальная форма обучения. Студент рассказывает свое решение преподавателю, отвечает на дополнительные вопросы.

Оценка успеваемости осуществляется по результатам: самостоятельного выполнения лабораторных работ, устного опроса при сдаче выполненных

самостоятельных заданий, индивидуальных лабораторных заданий и защиты групповых заданий, ответа на экзамене. Проверка индивидуальных заданий и устный опрос по их результатам позволяет проверить компетенции ПК-1, ПК-2, ПК-5. Существенным элементом образовательных технологий является не только умение студента найти решение поставленной задачи, но и донести его до всей аудитории. Защита групповых заданий проводится в виде представления результатов (средствами MS Office) и их обсуждения и служит контролем для проверки.

Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Перечень компетенций	Виды занятий					Формы контроля
	Л.	Лаб.	Пр.	КР	СРС	
ПК-1, ПК-2, ПК-5	+	+			+	– Защита группового задания
		+			+	– Опрос по результатам выполнения индивидуальных заданий; – Опрос по результатам самостоятельной работы;
		+			+	– Защита индивидуального задания

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

Структура оценочных средств для текущей и промежуточной аттестации

№ п/п	**Контролируемые разделы (темы) дисциплины**	**Код контролируемой компетенции (или ее части)**	**Наименование оценочного средства**	
			Текущий контроль	**Промежуточная аттестация**
1	Введение в информационную безопасность	ИПК-1.3 (D/01.6 У.1) ИПК-1.4 (A/01.6 У.1)	опрос по теме	*ВкЗ(1-2)*

2	Применение асимметричного шифрования.	ИПК-1.1 (D/29.7 Зн.8) ИПК-1.2 (A/01.6 Зн.1) ИПК-1.3 (D/01.6 У.1) ИПК-2.2	опрос по теме, *ЛР 1*	*ВкЗ(3)*
3	Безопасность контейнеров.	ИПК-1.1 (D/29.7 Зн.8) ИПК-1.2 (A/01.6 Зн.1) ИПК-1.3 (D/01.6 У.1) ИПК-1.4 (A/01.6 У.1) ИПК-1.5 (D/04.7 У.1) ИПК-1.7 (D/04.7 Тд.4) ИПК-1.8 (D/04.7 Тд.5)	опрос по теме, *ЛР 2*	*ВкЗ(4-7)*
4	Мониторинг, аудит, выявление аномалий и реагирование на инциденты в облачных средах.	ИПК-1.5 (D/04.7 У.1) ИПК-1.8 (D/04.7 Тд.5) ИПК-2.8 (D/01.6 У.1) ИПК-2.11 (D/29.7 У.2)	опрос по теме	*ВкЗ(8-9)*
5	WAF, DDoS	ИПК-1.7 (D/04.7 Тд.4) ИПК-1.8 (D/04.7 Тд.5) ИПК-5.7 (A/01.6 У.8)	опрос по теме, *ЛР 3*	*ВкЗ*(10-14*)*
6	ИИ и социальная инженерия	ИПК-1.4 (A/01.6 У.1) ИПК-1.5 (D/04.7 У.1) ИПК-2.18 (D/01.6 Тд.4)	опрос по теме	*ВкЗ*(15-18*)*
7	Правовые аспекты.	ИПК-1.5 (D/04.7 У.1) ИПК-1.7 (D/04.7 Тд.4) ИПК-2.1 (D/01.6 Зн.2)	опрос по теме	*ВкЗ*(19-20*)*
8	Популярные веб-уязвимости (языков программирования)	ИПК-2.2 (D/01.6 Зн.3) ИПК-2.8 (D/01.6 У.1)	опрос по теме, *ЛР 4*	*ВкЗ*(21-25*)*
9	Популярные веб-уязвимости (инфраструктуры)	ИПК-2.2 (D/01.6 Зн.3) ИПК-2.11 (D/29.7 У.2)	опрос по теме, *ЛР 6*	*ВкЗ*(27-30*)*
10	Популярные веб-уязвимости (фронтенд)	ИПК-2.1 (D/01.6 Зн.2) ИПК-2.2 (D/01.6 Зн.3), ИПК-2.8 (D/01.6 У.1)	опрос по теме, *ЛР 7*	*ВкЗ*(31-35*)*
11	Аутентификация и управление доступом: многофакторная аутентификация и IAM + OAuth/OIDC	ИПК-1.5 (D/04.7 У.1) ИПК-5.12 (D/04.7 Тд.5)	опрос по теме	*ВкЗ*(36-37*)*
12	Беспроводные сети	ИПК-1.5 (D/04.7 У.1), ИПК2.2 (D/01.6 Зн.3) ИПК-5.12 (D/04.7 Тд.5)	опрос по теме	*ВкЗ*(38-39*)*

Показатели, критерии и шкала оценки сформированных компетенций

Код и наименование компетенции	**Соответствие уровней освоения компетенции планируемым результатам обучения и критериям их оценивания**		
	пороговый	**базовый**	**продвинутый**
	Оценка		
	удовлетворительно	**хорошо**	**отлично**

Код и наименование компетенции	Соответствие уровней освоения компетенции планируемым результатам обучения и критериям их оценивания		
	пороговый	**базовый**	**продвинутый**
	Оценка		
	удовлетворительно	**хорошо**	**отлично**
ПК-1 Способен формулировать и решать актуальные и значимые задачи фундаментальной и прикладной математики ПК-2 Способен находить и извлекать актуальную научно-техническую информацию из электронных библиотек, реферативных журналов и т.п. ПК-5 Способен составлять и публично представлять научные обзоры, рефераты и отчеты по тематике проводимых исследований, а также подготовить научную публикацию	*Знать:* Основные виды сетевых, серверных и программных угроз. *Уметь:* Использовать открытые источники для поиска уязвимостей программного обеспечения (CVE) *Владеть:* Информацией по базовым сетевым атакам на программное обеспечение	*Знать:* Алгоритмы проверки облачной инфраструктуры *Уметь:* Использовать инструменты для автоматической проверки и анализа угроз информационной безопасности. *Владеть:* Правовыми аспектами информационной безопасности в законодательстве РФ.	*Знать*: Методы анализа сетевых угроз серверной облачной инфраструктуры. *Уметь*: Составлять отчеты о состоянии информационной инфраструктуры на основе анализа открытых источников (CVE) и информационных баз знаний. *Владеть*: Инструментами проектирования безопасной облачной инфраструктуры.

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерные задания на лабораторные работы

Примеры заданий:

1 Студенту предоставляется доступ к учебной виртуальной машине, имитирующей облачную виртуальную среду. Виртуальная машина содержит простое веб-приложение в Docker контейнере (nginx или fastAPI demo-app).

Используя инструменты (Trivy, Clair или др.), провести сканирование Docker-образа на наличие уязвимостей (CVEs) в базовом образе или зависимостях.

Необходимо составить отчет, включающий:

- Список найденных критических уязвимостей в базовом образе и зависимостях.

- Рекомендации по исправлению (обновление базового образа, патчинг зависимостей)
- Анализ конфигурации Dockerfile (привилегии пользователя, минимизация слоев, удаление ненужных пакетов)

2 Студенту дается описание веб-приложения (напр., интернет-магазин с API) и его архитектура в облаке.

Необходимо расписать технические решения по развертыванию приложения с учетом безопасности. Необходимо учитывать WAF, DDoS, мониторинг и реакции, возможные CVE.

4.2 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Перечень вопросов, выносимых на экзамен:

1 Основная цель атаки "Отказ в обслуживании" (DDoS)

2 Ключевое отличие угроз в облаке от традиционных

3 Протокол, использующий асимметричное шифрование для защищенного HTTPS

4 Уязвимость контейнеризации

5 Стандарт безопасности контейнеров

6 Инструменты сканирования образов на уязвимости

7 Защита от подмены реестра образов

8 Инструмент для агрегации логов в облаке

9 Действия при обнаружении компрометации облачного аккаунта

10 Основная задача WAF

11 Тип DDoS-атаки на уровень приложения

12 Облачные сервисы защиты от DDoS

13 Правило WAF для блокировки SQL-инъекций

14 Защита от атак на DNS

15 Использование ИИ для генерации фишинговых писем

16 Цель атаки "Pretexting"

17 Защита от целевого фишинга (spear phishing)

18 ИИ для обнаружения аномалий в поведении пользователя

19 Ключевой закон РФ о персональных данных

20 Регулятор ИБ критической инфраструктуры в РФ

21 Уязвимость выполнения произвольного SQL

22 Запуск ОС-команд через приложение

23 Недекларированная функциональность (Backdoor)

24 Использование устаревших/небезопасных библиотек

25 Небезопасная десериализация данных

26 Настройка прав доступа к облачному хранилищу (S3 Bucket Misconfig)

27 Открытые порты управления (SSH/RDP) в облаке

28 Уязвимость из-за необновленного ПО/ОС

29 Незащищенные ключи/токены в репозиториях

30 Отсутствие сегментации сети в облаке

31 Межсайтовое выполнение скриптов (XSS)

32 Подделка межсайтовых запросов (CSRF/XSRF)

33 Уязвимость включения сторонних ресурсов (CORS Misconfig / SSRF)

34 Небезопасное хранение данных в браузере (Local Storage / Cookie Flags)

35 Обход контроля доступа на клиенте (Broken Access Control - клиентская часть)

36 Методы обхода двухфакторной аутентификации

37 Безопасность JWT токенов

38 Методы перехвата пакетов беспроводной сети

39 Алгоритмы безопасности беспроводной сети WPA/WPA2

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

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

5.1 Основная литература:

1. Технологии обеспечения безопасности информационных систем : учебное пособие : [16+] / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов [и др.]. – Москва ; Берлин : Директ-Медиа, 2021. – 210 с. : ил., схем., табл. – Режим доступа: по подписке. – URL:

https://biblioclub.ru/index.php?page=book&id=598988 (дата обращения: 05.06.2025). – Библиогр.: с. 196-205. – ISBN 978-5-4499-1671-6. – DOI 10.23681/598988. – Текст : электронный.

2. Щерба, Е. В. Противодействие сетевым атакам в локальных сетях : учебное пособие : [16+] / Е. В. Щерба, М. В. Щерба, А. А. Магазев ; ред. О. В. Маер ; Омский государственный технический университет. – Омск : Омский государственный технический университет (ОмГТУ), 2021. – 119 с. : ил., табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=700833 (дата обращения: 05.06.2025). – Библиогр. в кн. – ISBN 978-5-8149-3250-1. – Текст : электронный.

3. Ларина, Т. Б. Администрирование операционных систем. Управление системой : учебное пособие для студентов направлений подготовки «Информатика и вычислительная техника» и «Информационная безопасность» : [16+] / Т. Б. Ларина ; Российский университет транспорта (РУТ (МИИТ)), Институт управления и информационных технологий, Кафедра «Вычислительные системы и сети». – Москва : Российский университет транспорта (РУТ (МИИТ)), 2020. – 72 с. : ил., таб. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=703233 (дата обращения: 05.06.2025). – Библиогр. в кн. – Текст : электронный.

Для освоения дисциплины инвалидами и лицами с ограниченными возможностями здоровья имеются издания в электронном виде в электронно-библиотечных системах.

5.2 Дополнительная литература:

1. Шилов, А. К. Управление информационной безопасностью : учебное пособие : [16+] / А. К. Шилов ; Южный федеральный университет, Институт компьютерных технологий и информационной безопасности. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2018. – 121 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=500065 (дата обращения: 05.06.2025). – Библиогр.: с. 81-82. – ISBN 978-5-9275-2742-7. – Текст : электронный.

2. А. С. Исмагилова, И. В. Салов, И. А. Шагапов, А. А. Корнилова, Информационная безопасность в цифровом обществе : учебное пособие : [16+] /; Башкирский государственный университет. – Уфа : Башкирский государственный университет, 2019. – 128 с. : табл., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=611084 (дата обращения: 05.06.2025). – Библиогр. в кн. – Текст : электронный.

1. Сидорова, Н. П. Операционные системы, среды и оболочки : практикум : учебное пособие : [16+] / Н. П. Сидорова, Г. Н. Исаева ; Технологический университет. – Москва : Директ-Медиа, 2022. – 51 с. : ил., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=693549 (дата обращения: 11.11.2024). – Библиогр.: с. 49. – ISBN 978-5-4499-3324-9. – DOI 10.23681/693549. – Текст : электронный.

2. Херинг, М. DevOps для современного предприятия : практическое пособие : [16+] / М. Херинг ; авт. предисл. Б. Гош ; пер. с англ. М. А. Райтман. – Москва : ДМК Пресс, 2020. – 234 с. : схем., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=596851 (дата обращения: 20.06.2024). – Библиогр. в кн. – ISBN 978-5-97060-836-4. – Текст : электронный..

3. Основы администрирования информационных систем : учебное пособие : [16+] / Д. О. Бобынцев, А. Л. Марухленко, Л. О. Марухленко [и др.]. – Москва ; Берлин : Директ-Медиа, 2021. – 202 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=598955 (дата обращения: 20.06.2024). – Библиогр. в кн. – ISBN 978-5-4499-1674-7. – DOI 10.23681/598955. – Текст : электронный.

4. Милл, И. Docker на практике : практическое пособие : [16+] / И. Милл, Э. Х. Сейерс ; пер. с англ. Д. А. Беликова. – Москва : ДМК Пресс, 2020. – 517 с. : схем., табл., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=686771 (дата обращения: 20.06.2024). – ISBN 978-5-97060-772-5. – Текст : электронный.

5. Форсгрен, Н. Ускоряйся! Наука DevOps : как создавать и масштабировать высокопроизводительные цифровые организации : практическое пособие : [16+] / Н. Форсгрен, Д. Хамбл, Д. Ким ; ред. Е. Закомурная ; пер. с англ. А. Техненко. – Москва : Альпина Паблишер, 2020. – 224 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=599299 (дата обращения: 20.06.2024). – ISBN 978-5-6042881-1-5. – Текст : электронный.

5.3. Интернет-ресурсы, в том числе современные профессиональные базы данных и информационные справочные системы

Электронно-библиотечные системы (ЭБС):

1. ЭБС «ЮРАЙТ» https://urait.ru/
2. ЭБС «УНИВЕРСИТЕТСКАЯ БИБЛИОТЕКА ОНЛАЙН» www.biblioclub.ru
3. ЭБС «BOOK.ru» https://www.book.ru
4. ЭБС «ZNANIUM.COM» www.znanium.com
5. ЭБС «ЛАНЬ» https://e.lanbook.com

Профессиональные базы данных:

1. Scopus http://www.scopus.com/
2. Научная электронная библиотека (НЭБ) http://www.elibrary.ru/
3. Springer Materials http://materials.springer.com/
4. zbMath https://zbmath.org/

5.4 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Перечень информационных технологий

– Проверка домашних заданий и консультирование посредством электронной почты.

– Использование электронных презентаций при проведении лекций и практических занятий.

6. Методические указания для обучающихся по освоению дисциплины

По курсу предусмотрено проведение лекционных занятий, на которых дается основной систематизированный материал, лабораторных работ, экзамена.

Важнейшим этапом курса является самостоятельная работа по дисциплине с использованием указанных литературных источников и методических указаний автора курса.

Виды и формы СР, сроки выполнения, формы контроля приведены выше в данном документе.

Для лучшего освоения дисциплины при защите ЛР студент должен ответить на несколько вопросов из лекционной части курса.

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная учебная работа (консультации) – дополнительное разъяснение учебного материала.

Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или лицом с ограниченными возможностями здоровья.

Выполненная магистрантом работа определяется на проверку преподавателю в установленные сроки. Если у преподавателя есть замечания, работа возвращается и после

исправлений либо вновь отправляется на проверку, если исправления существенные, либо предъявляется на зачете, где происходит ее защита.

7. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

№	Вид работ	Материально-техническое обеспечение дисциплины и оснащенность
1.	Лекционные занятия	Лекционная аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук), соответствующим программным обеспечением, а также необходимой мебелью (доска, столы, стулья). (аудитории: 129, 131, 133, А305, А307).
2.	Лабораторные занятия	Компьютерный класс, укомплектованный компьютерами с лицензионным программным обеспечением, необходимой мебелью (доска, столы, стулья). (аудитории: 101, 102, 106, 106а, 105/1, 107(2), 107(3), 107(5), А301).
3.	Групповые (индивидуальные) консультации	Аудитория для семинарских занятий, групповых и индивидуальных консультаций, укомплектованные необходимой мебелью (доска, столы, стулья). (аудитории: 129, 131).
4.	Текущий контроль, промежуточная аттестация	Аудитория для семинарских занятий, текущего контроля и промежуточной аттестации, укомплектованная необходимой мебелью (доска, столы, стулья) (аудитории: 129, 131, 133, А305, А307, 147, 148, 149, 150, 100С, А301б, А512), компьютерами с лицензионным программным обеспечением и выходом в интернет (106, 106а, А301)
5.	Самостоятельная работа	Кабинет для самостоятельной работы, оснащенный компьютерной техникой с возможностью подключения к сети «Интернет», программой экранного увеличения, обеспеченный доступом в электронную информационно-образовательную среду университета, необходимой мебелью (доска, столы, стулья). (Аудитория 102а, читальный зал).

Примечание: Конкретизация аудиторий и их оснащение определяется ОПОП.