

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Б1.О.21
(индекс дисциплины)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Обеспечение безопасности при разработке программного обеспечения

(наименование дисциплины)

по направлению подготовки
38.03.05 Бизнес-информатика

направленность (профиль)
Медиа-арт и анимация

Форма обучения: очная

Год набора: 2024

Общая трудоемкость: 5 ЗЕ

Распределение часов дисциплины по семестрам

Семестр	7	Итого
Форма контроля	экзамен	
Вид занятий		
Лекции	16	16
Лабораторные		
Практические	32	32
Руководство: курсовые работы (проекты) / РГР		
Промежуточная аттестация		
Контактная работа	48.35	48.35
Самостоятельная работа	96	96
Контроль	35.65	35.65
Итого	180	180

Рабочую программу составил:
доцент кафедры «Прикладная математика и информатика», канд. экон. наук, Раченко Т.А.

(должность, ученое звание, степень, Фамилия И.О.)

Рецензирование рабочей программы дисциплины:



Отсутствует



Рецензент

(должность, ученое звание, степень, Фамилия И.О.)

Рабочая программа составлена на основании ФГОС ВО и учебного плана направления подготовки

09.03.03 Прикладная информатика

(код и наименование направления подготовки, специальности в соответствии с ФГОС ВПО)

Срок действия рабочей программы дисциплины до «31» августа 2029 г.

СОГЛАСОВАНО

Директор

Центра креативных индустрий

«__» _____ 20__ г.

(подпись)

_____ А.В.Зуев _____
(И.О. Фамилия)

УТВЕРЖДЕНО

На заседании кафедры «Прикладная математика и информатика»

(протокол заседания № 1 от 28» августа 2024 г.).

1. Цель освоения дисциплины

Цель – формирование у обучающихся компетенций в области разработки безопасного программного обеспечения, методов и средств защиты информации в программных системах.

Задачи:

1. Изучение типовых уязвимостей программного обеспечения и методов их предотвращения.
2. Знакомство с принципами проектирования безопасного программного обеспечения.
3. Изучение методов и средств аутентификации и авторизации пользователей.
4. Знакомство с криптографическими методами и средствами защиты данных.
5. Изучение протоколов безопасной передачи данных.
6. Изучение методов обеспечения целостности данных.
7. Освоение навыков использования инструментальных средств обеспечения безопасности программного обеспечения.
8. Формирование умения анализировать уязвимости программного обеспечения и разрабатывать политику информационной безопасности.
9. Овладение приемами предотвращения, обнаружения и нейтрализации угроз безопасности программных систем.

2. Место дисциплины (учебного курса) в структуре ОПОП ВО

Дисциплины, учебные курсы, на освоении которых базируется данная дисциплина (учебный курс) – Информационные системы и технологии, Базы данных и управление данными.

Дисциплины, учебные курсы, для которых необходимы знания, умения, навыки, приобретаемые в результате изучения данной дисциплины (учебного курса) – Выполнение и защита выпускной квалификационной работы.

3. Планируемые результаты обучения

Формируемые и контролируемые компетенции (код и наименование)	Индикаторы достижения компетенций (код и наименование)	Планируемые результаты обучения
ОПК -3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;	ОПК-3.1. Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	Знать: методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности Уметь: применять методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности Владеть: навыками применения методов и средств решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
	ОПК-3.2. Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	Знать: стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности Уметь: применять стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности Владеть: навыками применения стандартных задач профессиональной деятельности на основе информацион-

Формируемые и контролируемые компетенции (код и наименование)	Индикаторы достижения компетенций (код и наименование)	Планируемые результаты обучения
		ной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
	ОПК-3.3. Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.	<p>Знать: принципы подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом</p> <p>Уметь: составлять обзоры, аннотации, рефераты, научные доклады, публикации, и библиографии по научно-исследовательской работе с учетом</p> <p>Владеть: навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом</p>

4. Структура и содержание дисциплины

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
1. Основные понятия и определения безопасности информации. Требования безопасности разработки программного обеспечения	Лек1	Тема 1. Введение в безопасность при разработке программного обеспечения	7	2	-	-	Собеседование (устный опрос)
	Ср	Изучение лекционного материала и подготовка к практическим занятиям	7	10	-	-	
	Лек2	Тема 1.1. Методы оптимизации управления жизненным циклом распределенных данных с учетом информационной безопасности	7	2	-	-	Собеседование (устный опрос)
	Ср	Изучение лекционного материала и подготовка к практическим занятиям	7	20	-	-	
2. Сетевые технологии и информационная безопасность	Лек3	Тема 2. Принципы информационной безопасности. Проектирование безопасности	7	2	-	-	Собеседование (устный опрос)
	Пр1	Тема 1 План управления жизненным циклом данных для конкретного проекта	7	2	-	-	Отчет по практической работе (защита)
	Пр2	Тема 1 План управления жизненным циклом данных для конкретного проекта	7	2	-	-	
	Пр3	Тема 1 План управления жизненным циклом данных для конкретного проекта	7	2	-	-	
	Пр4	Тема 1 План управления жизненным циклом данных для конкретного проекта	7	2	-	-	
	Пр5	Тема 1 План управления жизненным циклом данных для конкретного проекта	7	2	-	-	
	Пр6	Тема 2 Анализ и оценка угроз безопасности данных проекта	7	2	-	-	Отчет по практической работе (защита)
	Пр7	Тема 2 Анализ и оценка угроз безопасности	7	2	-	-	

	данных проекта						
Пр8	Тема 2 Анализ и оценка угроз безопасности данных проекта	7	2	-	-		
Пр9	Тема 3 Проектирование системы защиты дан-ных	7	2	-	-	Отчет по практической работе (защита)	
Пр10	Тема 3 Проектирование системы защиты дан-ных	7	2	-	-		
Пр11	Тема 3 Проектирование системы защиты дан-ных	7	2	-	-		
Пр12	Тема 3 Проектирование системы защиты дан-ных	7	2	-	-		
Пр13	Тема 3 Проектирование системы защиты дан-ных	7	2		-		
Пр14	Тема 4 Реализация системы защиты данных	7	2	-	-	Отчет по практической работе (защита)	
Пр15	Тема 4 Реализация системы защиты данных	7	2	-			
Пр16	Тема 5 Тестирование и анализ эффективности примененных мер по обеспечению безопасно-сти данных	7	2	-	-	Отчет по практической работе (защита)	
Ср	Изучение лекционного материала и подготов-ка к практическим занятиям	7	16	-	-		
Лек4	Тема 3. Технология осуществления оптимиза-ции управления жизненным циклом распре-деленных данных с учетом информационной безопасности. Разработка безопасности	7	2	-	-	Собеседование (устный опрос)	
Ср	Изучение лекционного материала и подготов-ка к практическим занятиям	7	4	-	-		
Лек5	Тема 4. Инструменты, используемые для обеспечения безопасности на этапе разра-ботки	7	2	-	-	Собеседование (устный опрос)	
Ср	Изучение лекционного материала и подготов-ка к практическим занятиям	7	10	-	-		
3. Разработка при-	Лек6	Тема 5. Оптимизации управления жизненным	7	2	-	-	Собеседование (устный

кладных задач с учетом требований безопасности		циклом распределенных данных с учетом информационной безопасности. Обслуживание безопасности					опрос)
	Ср	Изучение лекционного материала и подготовка к практическим занятиям	7	4	-	-	
	Лек7	Тема 6. Угрозы безопасности и методы их предотвращения	7	2	-	-	Собеседование (устный опрос)
	Ср	Изучение лекционного материала и подготовка к практическим занятиям	7	10	-	-	
	Лек8	Тема 7. Реагирование на угрозы безопасности	7	2	-	-	Собеседование (устный опрос)
	Ср	Изучение лекционного материала и подготовка к практическим занятиям	7	22	-	-	
	ПА	Промежуточная аттестация	7	0,35	-	-	
	Контроль	Зачет	7	35,65	-	-	Оценка уровня знаний и умений обучающихся по дисциплине на основе ответов на вопросы из билетов
Итого				180			

5. Образовательные технологии

В рамках изучения дисциплины предусмотрено использование следующих образовательных технологий:

- технология традиционного обучения;
- интерактивные технологии: учебные дискуссии (применяются во всех модулях по итогам выполнения работ).

Технологии традиционного обучения - организация учебного процесса в вузе, основанная на лекционных и практических формах обучения: объяснительно-иллюстративное обучение. Данная технология применяется во всех модулях курса.

Технология интерактивного обучения — это организация учебного процесса, которая предполагает максимальную активность обучающихся в процессе формирования ключевых компетенций. На учебной дискуссии обучающиеся представляют результаты выполнения заданной работы. Проводится обсуждение применённых решений, их эффективности и архитектуры программного кода.

6. Методические указания по освоению дисциплины

6.1 Рекомендации по подготовке к практическим занятиям

Обучающимся следует:

- при подготовке к занятиям обязательно использовать не только учебную литературу, но и другие источники;
- в начале занятий задать преподавателю вопросы по материалу, вызвавшему затруднения в его понимании и освоении при решении задач, заданных для самостоятельного решения;
- на занятии доводить каждую задачу до окончательного решения, демонстрировать понимание путей решения поставленных задач и освоения выданных знаний, в случае затруднений обращаться к преподавателю.

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса. Если обучающийся видит несколько путей решения задачи, то нужно сравнить их и выбрать самый рациональный. Полезно до начала решения задачи составить краткий план решения задачи. Решение проблемных задач или примеров следует излагать подробно, отделяя вспомогательные пути решения от основных. Решения при необходимости нужно сопровождать комментариями, схемами, алгоритмами.

Следует помнить, что решение каждой учебной задачи должно доводиться до окончательного логического ответа, которого требует условие, и по возможности с выводом. Полученный ответ следует проверить способами, вытекающими из существа данной задачи. Полезно также (если возможно) решать несколькими способами и сравнить полученные результаты. Решение задач данного типа нужно продолжать до приобретения твердых навыков в их решении.

6.2 Рекомендации по подготовке к итоговой сдаче дисциплины

Подготовка к итоговой сдаче предмета способствует закреплению, углублению и обобщению знаний, получаемых, в процессе обучения, а также применению их к решению практических задач. Готовясь к ней, обучающийся ликвидирует имеющиеся пробелы в знаниях, углубляет, систематизирует и упорядочивает свои знания. На итоговой сдаче обучающийся демонстрирует то, что он приобрел в процессе обучения по конкретной учебной дисциплине.

Необходимо ориентировать обучающихся на систематическую подготовку к занятиям в течение семестра, что позволит использовать время экзаменационной сессии для систематизации знаний.

7. Оценочные средства

7.1 Паспорт оценочных средств экзамену

Семестр	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
7	ОПК-3	Тестовые задания по лекционному материалу. Вопросы к экзамену. Отчеты по практическим работам 1-5

7.2 Типовые задания или иные материалы, необходимые для текущего контроля

7.2.1 Вопросы для собеседования по модулю

Типовые примеры заданий

Модуль 1. Основные понятия и определения безопасности информации. Требования безопасности разработки программного обеспечения

1. Какие основные понятия и определения безопасности информации необходимо знать при разработке программного обеспечения, и как они связаны с управлением жизненным циклом распределенных данных?
2. Какие требования безопасности необходимо учитывать при разработке программного обеспечения, и как они связаны с оптимизацией управления жизненным циклом распределенных данных?
3. Какие методы оптимизации управления жизненным циклом распределенных данных существуют, и какие из них наиболее эффективны с точки зрения безопасности информации?
4. Какие риски связанные с безопасностью данных могут возникнуть при разработке программного обеспечения, и как их можно предотвратить?
5. Какие принципы информационной безопасности необходимо учитывать при разработке программного обеспечения, и как они связаны с управлением жизненным циклом распределенных данных?
6. Какие методы обеспечения безопасности данных можно использовать при разработке программного обеспечения, и как они связаны с управлением жизненным циклом распределенных данных?
7. Какие принципы управления жизненным циклом распределенных данных следует учитывать при разработке программного обеспечения, и как они связаны с безопасностью информации?
8. Как оценить уровень безопасности разработанного программного обеспечения, и какие методы использовать для его улучшения?
9. Какие методы выбора оптимального метода управления жизненным циклом распределенных данных вы можете порекомендовать обучающимся при разработке программного обеспечения?
10. Какие методы обнаружения и предотвращения уязвимостей в программном обеспечении существуют, и как они связаны с безопасностью данных и управлением жизненным циклом распределенных данных?

11. Какие методы защиты данных можно использовать при работе с базами данных, и как они связаны с управлением жизненным циклом распределенных данных и безопасностью информации?
12. Какие методы защиты данных можно использовать при работе с облачными сервисами, и как они связаны с управлением жизненным циклом распределенных данных и безопасностью информации?
13. Какие методы защиты данных можно использовать при работе с виртуальными частными сетями (VPN), и как они связаны с управлением жизненным циклом распределенных данных и безопасностью информации?
14. Какие методы обеспечения безопасности данных можно использовать при работе с системами управления контентом, и как они связаны с управлением жизненным циклом распределенных данных и безопасностью информации?
15. Какие методы обеспечения безопасности данных можно использовать при работе с веб-серверами, и как они связаны с управлением жизненным циклом распределенных данных и безопасностью информации?

Модуль 2. Сетевые технологии и информационная безопасность

1. Какие принципы информационной безопасности необходимо учитывать при работе с сетевыми технологиями, и как они связаны с управлением жизненным циклом распределенных данных?
2. Какие методы оптимизации управления жизненным циклом распределенных данных существуют, и какие из них наиболее эффективны с точки зрения безопасности информации?
3. Какие риски связанные с безопасностью данных могут возникнуть при работе с сетевыми технологиями, и как их можно предотвратить?
4. Какие методы обеспечения безопасности данных можно использовать при работе с сетевыми технологиями, и как они связаны с управлением жизненным циклом распределенных данных?
5. Какие принципы управления жизненным циклом распределенных данных необходимо учитывать для обеспечения безопасности информации при работе с сетевыми технологиями?
6. Какие методы выбора оптимального метода управления жизненным циклом распределенных данных для обеспечения безопасности информации вы можете порекомендовать обучающимся?
7. Какие методы защиты данных можно использовать при работе с беспроводными сетями, и как они связаны с управлением жизненным циклом распределенных данных?
8. Какие методы обеспечения безопасности данных можно использовать при работе с сетевыми протоколами, и как они связаны с управлением жизненным циклом распределенных данных?
9. Какие методы защиты данных можно использовать при работе с веб-серверами, и как они связаны с управлением жизненным циклом распределенных данных?
10. Какие принципы информационной безопасности следует учитывать при разработке сетевых приложений, и как они связаны с управлением жизненным циклом распределенных данных?
11. Какие методы оптимизации управления жизненным циклом распределенных данных можно использовать при разработке сетевых приложений, и какие принципы безопасности данных следует учитывать?
12. Какие методы защиты данных можно использовать при работе с базами данных, и как они связаны с управлением жизненным циклом распределенных данных?

13. Какие методы защиты данных можно использовать при работе с облачными сервисами, и как они связаны с управлением жизненным циклом распределенных данных?
14. Какие методы защиты данных можно использовать при работе с виртуальными частными сетями (VPN), и как они связаны с управлением жизненным циклом распределенных данных?
15. Какие методы обеспечения безопасности данных можно использовать при работе с системами управления контентом, и как они связаны с управлением жизненным циклом распределенных данных?

Модуль 3. Разработка прикладных задач с учетом требований безопасности

1. Какие методы оптимизации управления жизненным циклом распределенных данных существуют, и какие из них наиболее эффективны с точки зрения безопасности информации?
2. Какие риски связанные с безопасностью данных могут возникнуть при разработке прикладных задач, и как их можно предотвратить?
3. Какие принципы информационной безопасности необходимо учитывать при разработке прикладных задач, и как они могут быть реализованы?
4. Какие методы обеспечения безопасности данных можно использовать при разработке прикладных задач?
5. Какие принципы управления жизненным циклом распределенных данных необходимо учитывать для обеспечения безопасности информации?
6. Какие методы выбора оптимального метода управления жизненным циклом распределенных данных вы можете порекомендовать обучающимся?
7. Какие принципы информационной безопасности следует учитывать при разработке приложений для мобильных устройств, и как это связано с управлением жизненным циклом распределенных данных?
8. Какие риски связанные с безопасностью данных могут возникнуть при использовании облачных сервисов, и как их можно предотвратить?
9. Какие методы обеспечения безопасности данных можно использовать при работе с облачными сервисами, и как они связаны с управлением жизненным циклом распределенных данных?
10. Какие принципы управления жизненным циклом распределенных данных следует учитывать при разработке систем электронного документооборота, и как они связаны с безопасностью информации?
11. Какие методы оптимизации управления жизненным циклом распределенных данных можно использовать при работе с системами управления проектами, и какие принципы безопасности данных следует учитывать?
12. Какие методы защиты данных можно использовать при работе с мобильными приложениями, и как они связаны с управлением жизненным циклом распределенных данных?
13. Какие методы обеспечения безопасности данных можно использовать для защиты от кибератак, и как они связаны с управлением жизненным циклом распределенных данных?
14. Какие методы защиты данных можно использовать при работе с системами управления контентом, и как они связаны с управлением жизненным циклом распределенных данных?
15. Какие методы защиты данных можно использовать при работе с системами управления ресурсами предприятия, и как они связаны с управлением жизненным циклом распределенных данных?

Критерии оценки:

Раскрытие 90-100% ответа на вопрос - 20 баллов; раскрытие 80-89% ответа на вопрос - 18 баллов; раскрытие 66-79% ответа на вопрос - от 15 баллов; раскрытие 50-65% ответа на вопрос - от 12 баллов; раскрытие менее 50% ответа на вопрос - от 0 до 11 баллов.

7.2.2 Комплект отчетов по практическим работам (примеры)

Типовые примеры заданий

Практическое занятие №1 «План управления жизненным циклом данных для конкретного проекта»

Форма отчета по практическому занятию №1

- титульный лист;
- задание;
- результат выполнения задания;
- результат эксперимента (таблицы и графики);
- выводы по работе.

Практическое занятие №2 «Анализ и оценка угроз безопасности данных проекта»

Форма отчета по практическому занятию №2

- титульный лист;
- задание;
- результат выполнения задания;
- результат эксперимента (таблицы и графики);
- выводы по работе.

Практическое занятие №3 «Проектирование системы защиты данных»

Форма отчета по практическому занятию №3

- титульный лист;
- задание;
- результат выполнения задания;
- результат эксперимента (таблицы и графики);
- выводы по работе.

Практическое занятие №4 «Реализация системы защиты данных»

Форма отчета по практическому занятию №4

- титульный лист;
- задание;
- результат выполнения задания;
- результат эксперимента (таблицы и графики);
- выводы по работе.

Практическое занятие №5 «Тестирование и анализ эффективности примененных мер по обеспечению безопасности данных»

Форма отчета по практическому занятию №5

- титульный лист;
- задание;
- результат выполнения задания;
- результат эксперимента (таблицы и графики);
- выводы по работе.

Требования к оформлению

Отчет должен содержать подробное описание (включая иллюстративный материал) последовательности действий проделанных обучающийся для выполнения заданий. Оформление отчета должно соответствовать методическому указанию рекомендациям, изложенным учебно-методическом пособии [Очеповский А.В. Общие требования по выполнению и

оформлению контрольных, курсовых и выпускных квалификационных работ : Учебно-методическое пособие. – Тольятти : ТГУ, 2015. 78 с.].

Процедура оценивания

Оценка выполненной работы проводится по критериям:

1. Наличие всей существенной информации по работе
2. Точность и полнота предоставляемых сведений
3. Непротиворечивость приводимой информации
4. Правильность интерпретаций и выводов, которые сделаны по результатам работы
5. Степень достижения обучающимся поставленной цели
6. Обоснованность применяемого решения
7. Грамотность (содержательная) используемых формулировок

Оценка:

- **«Зачтено»:** отчет соответствует большинству или всем критериям, демонстрирует понимание темы и умение применять полученные знания на практике.
- **«Не зачтено»:** отчет не соответствует ключевым критериям, содержит значительные недостатки в содержании, структуре или оформлении.

7.3. Оценочные средства для промежуточной аттестации по итогам освоения дисциплины

7.3.1

Вопросы к промежуточной аттестации (экзамену)

1. Что такое оптимизация управления жизненным циклом распределенных данных?
2. Какие методы оптимизации управления жизненным циклом распределенных данных вы знаете?
3. Какие принципы информационной безопасности необходимо учитывать при разработке программного обеспечения?
4. Что такое угрозы информационной безопасности?
5. Какие методы информационной безопасности вы знаете?
6. Какие технологии могут быть использованы для оптимизации управления жизненным циклом распределенных данных?
7. Какие принципы информационной безопасности необходимо учитывать при оптимизации управления жизненным циклом распределенных данных?
8. Какие риски связанные с безопасностью данных могут возникнуть в процессе разработки программного обеспечения?
9. Какие меры безопасности могут быть приняты для защиты данных в процессе разработки программного обеспечения?
10. Какие методы обеспечения безопасности данных можно использовать при работе с распределенными системами?
11. Что такое жизненный цикл распределенных данных?
12. Какие этапы включает жизненный цикл распределенных данных?
13. Какие принципы управления жизненным циклом распределенных данных следует учитывать для обеспечения безопасности информации?
14. Какие методы выбора оптимального метода управления жизненным циклом распределенных данных вы знаете?
15. Какой метод оптимизации управления жизненным циклом распределенных данных вы считаете самым эффективным и почему?

16. Какие методы обеспечения безопасности данных вы считаете наиболее эффективными?
17. Какие принципы управления жизненным циклом распределенных данных следует учитывать при разработке приложений для мобильных устройств?
18. Какие принципы информационной безопасности следует учитывать при работе с облачными сервисами?
19. Какие риски связанные с безопасностью данных могут возникнуть при использовании облачных сервисов?
20. Какие методы обеспечения безопасности данных можно использовать при работе с облачными сервисами?
21. Какие принципы управления жизненным циклом распределенных данных следует учитывать при разработке систем электронного документооборота?
22. Какие методы оптимизации управления жизненным циклом распределенных данных можно использовать при работе с системами электронного документооборота?
23. Что такое криптография и как она может быть использована для обеспечения безопасности данных?
24. Какие методы криптографии вы знаете?
25. Какие принципы криптографии необходимо учитывать при защите данных?
26. Какие методы аутентификации пользователей можно использовать при работе с распределенными системами?
27. Какие методы обнаружения и предотвращения атак на программное обеспечение вы знаете?
28. Какие методы защиты от вредоносных программ можно использовать при разработке программного обеспечения?
29. Какие принципы безопасности данных следует учитывать при работе с интернет-приложениями?
30. Какие методы обеспечения безопасности данных можно использовать для защиты от кибератак?
31. Какие принципы управления жизненным циклом распределенных данных следует учитывать при разработке систем управления проектами?
32. Какие методы оптимизации управления жизненным циклом распределенных данных можно использовать при работе с системами управления проектами?
33. Какие принципы информационной безопасности необходимо учитывать при разработке систем управления проектами?
34. Какие методы защиты данных можно использовать при работе с мобильными приложениями?
35. Какие принципы управления жизненным циклом распределенных данных следует учитывать при разработке систем электронной коммерции?
36. Какие методы оптимизации управления жизненным циклом распределенных данных можно использовать при работе с системами электронной коммерции?
37. Какие методы защиты данных можно использовать при работе с системами электронной коммерции?
38. Какие принципы информационной безопасности следует учитывать при работе с системами управления контентом?
39. Какие методы оптимизации управления жизненным циклом распределенных данных можно использовать при работе с системами управления контентом?
40. Какие методы защиты данных можно использовать при работе с системами управления контентом?
41. Какие принципы управления жизненным циклом распределенных данных следует учитывать при работе с системами бизнес-аналитики?
42. Какие методы оптимизации управления жизненным циклом распределенных данных можно использовать при работе с системами бизнес-аналитики?

43. Какие методы защиты данных можно использовать при работе с системами бизнес-аналитики?
44. Какие принципы информационной безопасности следует учитывать при работе с системами управления производственными данными?
45. Какие методы оптимизации управления жизненным циклом распределенных данных можно использовать при работе с системами управления производственными данными?
46. Какие методы защиты данных можно использовать при работе с системами управления производственными данными?
47. Какие принципы управления жизненным циклом распределенных данных следует учитывать при работе с системами управления ресурсами предприятия?
48. Какие методы оптимизации управления жизненным циклом распределенных данных можно использовать при работе с системами управления ресурсами предприятия?
49. Какие методы защиты данных можно использовать при работе с системами управления ресурсами предприятия?
50. Какие принципы информационной безопасности следует учитывать при работе с системами управления проектами?
51. Что такое репликация данных и как она влияет на производительность распределенных систем?
52. Какие алгоритмы согласованности данных (Consistency Models) используются в распределенных системах?
53. Как CAP-теорема влияет на проектирование распределенных баз данных?
54. Какие преимущества и недостатки у шардирования данных?
55. Как работает механизм кэширования в распределенных системах и какие технологии для этого используются?
56. Какие методы балансировки нагрузки применяются в распределенных системах?
57. Что такое Eventual Consistency и в каких системах она применяется?
58. Какие инструменты мониторинга данных используются в распределенных системах?
59. Как обеспечивается отказоустойчивость в распределенных системах?
60. Какие стандарты и фреймворки регулируют управление жизненным циклом данных (например, GDPR, ISO 27001)?
61. Как машинное обучение может использоваться для оптимизации управления данными?
62. Какие проблемы безопасности возникают при использовании edge computing?
63. Как работает Zero Trust Security Model и как его применить к распределенным данным?
64. Какие методы защиты от инсайдерских угроз существуют?
65. Как обеспечивается безопасность данных в микросервисной архитектуре?
66. Какие методы анонимизации данных используются для защиты конфиденциальности?
67. Как blockchain может быть использован для обеспечения целостности данных?
68. Какие методы защиты от SQL-инъекций и NoSQL-инъекций вы знаете?
69. Как работают системы обнаружения аномалий (Anomaly Detection) в распределенных системах?
70. Какие best practices по безопасности данных в DevOps (DevSecOps)?

7.3.2 Критерии и нормы оценки

Ответы на вопросы билета обеспечивают возможность адекватной оценки знаний и профессиональной подготовки бакалавров. Важным фактором при этом является умение экзаменуемого оперировать в своем ответе ссылками на соответствующие положения учебной и научной литературы. По результатам выполнения практического задания определяется уровень сформированности профессиональных компетенций обучающимся по использованию современных технологий решения прикладных задач предметной области.

Требования к ответу:

- ответ должен быть научным, логически стройным, опираться на соответствующие теоретические положения и концепции;
- ответ следует строить в единстве теории и практики с подтверждением теоретических положений реальными практическими примерами;
- практические задания должны быть выполнены на компьютере с использованием соответствующих программных средств.

Оценивание:

- порядок ответов на вопросы билета определяется самим обучающимся;
- при необходимости дополнительные вопросы задаются обучающемуся после ответа на все три вопроса билета;
- оценка результатов производится по четырехбалльной системе («отлично», «хорошо», «удовлетворительно», «неудовлетворительно»);
- оценка объявляется после завершения ответа обучающегося на дополнительные вопросы.

Критерии оценки:

- оценка «отлично» выставляется обучающемуся, если он исчерпывающе и грамотно дал ответы на вопросы экзаменационного билета или при ответе допустил небольшую неточность на 1 вопрос, но при этом смог грамотно ответить на дополнительные вопросы;
- оценка «хорошо» выставляется обучающемуся, если он исчерпывающе и грамотно дал ответ на 1 вопрос экзаменационного билета, а на другой только тезисные высказывания или допустил небольшие неточности при ответе на вопросы экзаменационного билета и дал краткие ответы на дополнительные вопросы;
- оценка «удовлетворительно» выставляется обучающемуся, если он не смог дать ответ на один из вопросов экзаменационного билета или ответил на все вопросы, но при этом ответы содержали только тезисные высказывания;
- оценка «неудовлетворительно» выставляется обучающемуся, если он не дал ответ на вопросы экзаменационного билета или в ответе содержались фундаментальные ошибки.

8. Учебно-методическое и информационное обеспечение дисциплины

8.1 Обязательная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно-методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
1	Баранова Е. К.	Криптографические методы защиты информации : лаб. практикум : учеб. пособие / Е. К. Баранова, А. В. Бабаш. - Москва : КноРус, 2015. - 196 с. : ил. + CD. - (Бакалавриат). - Библиогр. в конце гл. - ISBN 978-5-406-03802-4 : 250-00. - ISBN 205-00.	Учебное пособие	2015	2
2	Фороузан Б. А.	Криптография и безопасность сетей [Электронный ресурс] : учеб. пособие / Б. А. Фороузан ; пер. с англ. под ред. А. Н. Берлина . - Москва : ИНТУИТ, 2017 ; Саратов : Вузовское образование, 2017. - 782 с. : ил. - (Основы информационных технологий). - ISBN 978-5-4487-0143-6.	Учебное пособие	2017	ЭБС «IPRbooks»
3	Хорев П. Б.	Программно-аппаратная защита информации [Электронный ресурс] : учеб. пособие / П. Б. Хорев. - 2-е изд., испр. и доп. - Москва : Форум : ИНФРА-М, 2015. - 352 с. - (Высшее образование). - ISBN 978-5-00091-004-7.	Учебное пособие	2015	ЭБС «Znanium.com»
4	Раченко. Т.А.	Раченко. Т.А. Информационная безопасность : электронное учебно-методическое пособие / Т.А. Раченко. – Тольятти : Изд-во ТГУ, 2024. – 1 оптический диск. – ISBN 978-5-8259-1612-5	Учебно-методическое пособие	2024	Репозиторий ТГУ

8.2 Дополнительная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно-методиче- ское пособие, практикум, др.)	Год из- дания	Количество в научной биб- лиотеке / Наименова- ние ЭБС
1	Кукина Е. Г.	Введение в криптографию [Электронный ресурс] : сборник задач и упражнений / Е. Г. Кукина, В. А. Романьков. - Омск : ОмГУ, 2013. - 91 с. - ISBN 978-5-7779-1588-7.	Учебное пособие	2013	ЭБС «IPRbooks»
2	Никифоров С. Н.	Защита информации [Электронный ресурс] : учеб. пособие / С. Н. Никифоров. - Санкт-Петербург : СПбГАСУ, 2015. - 383 с. : ил. - ISBN 978-5-9227-0585-1.	Учебное пособие	2015	ЭБС «IPRbooks»
3	Спицын В. Г.	Информационная безопасность вычислительной техники [Электронный ресурс] : учебное пособие / В. Г. Спицын. - Томск : Эль Контент, 2011. - 148 с. - ISBN 978-5-4332-0020-3.	Учебное пособие	2011	ЭБС «IPRbooks»
4	Федин Ф. О.	Информационная безопасность [Электронный ресурс] : учебное пособие / Ф. О. Федин, В. П. Офицеров, Ф. Ф. Федин ; [под ред. В. А. Дикарева]. - Москва : МГПУ, 2011. - 260 с.	Учебное пособие	2011	ЭБС «IPRbooks»

8.3 Перечень профессиональных баз данных и информационных справочных систем

№ п/п	Наименование	Ссылка
1	Springer Nature (Полнотекстовая коллекция журналов)	https://www.springernature.com/gp/products
2	Springer eBooks (Полнотекстовая коллекция электронных книг издательства Springer Nature)	https://link.springer.com/
3	«Кодекс»	https://kodeks.ru/
4	Техэксперт	https://cntd.ru/

8.4 Перечень программного обеспечения

№ п/п	Наименование ПО	Количество лицензий	Реквизиты договора (дата, номер, срок действия)
1	Visual Studio Code (VS Code)	неограниченный	Бесплатное ПО, лицензия MIT
2	Eclipse IDE	неограниченный	Бесплатное ПО, лицензия Eclipse Public License (EPL)
3	JUnit	неограниченный	Бесплатное ПО, лицензия Eclipse Public License (EPL)
4	SonarQube	неограниченный	Бесплатное ПО, лицензия GNU LGPL
5	Git	неограниченный	Бесплатное ПО, лицензия GPLv2
6	GitHub	неограниченный	Бесплатное ПО, лицензия MIT
7	OWASP ZAP (Zed Attack Proxy)	неограниченный	Бесплатное ПО, лицензия Apache License 2.0
8	Wireshark	неограниченный	Бесплатное ПО, лицензия GPLv2

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

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий	Перечень основного оборудования
1	Компьютерный класс. Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для проведения лабораторных работ. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для прове-	Компьютер (монитор 17", системный блок Intel (R) Celeron (R) 2,66 GHz / 1 Gb / 80 Gb), маршрутизатор 2801 Router, коммутатор Catalyst, экран / интер-

	дения групповых и индивидуальных консультаций Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации. (УЛК-408).	активная доска Smart Board ТВ, проектор Acer P1303W, стол преподавательский, столы ученические, столы компьютерные, стулья, доска аудиторная (маркерная).
2	Помещение для самостоятельной работы обучающихся (УЛК-105).	Стол, стулья, стеллажи (в т.ч. выставочные) с книгами, компьютеры, мобильные рабочие места.
3	Помещение для самостоятельной работы обучающихся (УЛК-406).	Стол компьютерный, стулья, микрокомпьютеры raspberry pi 32 bit.