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

Б1.В.08
(индекс дисциплины)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Обеспечение безопасности при разработке программного обеспечения
(наименование дисциплины)

по направлению подготовки (специальности)

09.03.03 Прикладная информатика
(код и наименование направления подготовки, специальности в соответствии с ФГОС ВПО/ФГОС ВО)

Разработка программного обеспечения
(направленность (профиль))

Форма обучения: заочная

Год набора: 2019

Общая трудоемкость: **3 ЗЕ**

Распределение часов дисциплины по семестрам

Семестр	**4**	**Итого**
Форма контроля / **Вид занятий**	зачет	
Лекции	**4**	**4**
Лабораторные		
Практические	**4**	**4**
Руководство: курсовые работы (проекты) / РГР		
Промежуточная аттестация	**0,25**	**0,25**
Контактная работа	**8,25**	**8,25**
Самостоятельная работа	**96**	**96**
Контроль	**3,75**	**3,75**
Итого	**108**	**108**

Рабочую программу составил:
доцент кафедры «Прикладная математика и информатика» доцент к.э.н. 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 (специальности)

09.03.03 Прикладная информатика

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

Срок действия рабочей программы дисциплины до «31» декабря 2024 г.

УТВЕРЖДЕНО

На заседании кафедры «Прикладная математика и информатика»
(протокол заседания № 6 от «19» декабря 2018 г.).

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 0101AEC60064AF94AD41EA4854441FD671
Владелец: Гущина Оксана Михайловна
Действителен: с 07.12.2022 до 07.12.2023

1. Цель освоения дисциплины

Цель – формирование у студентов 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

Данная дисциплина (учебный курс) относится к блоку В - Часть, формируемая участниками образовательных отношений

Дисциплины, учебные курсы, на освоении которых базируется данная дисциплина (учебный курс) – Информационные системы и технологии, Управление проектами разработки программного обеспечения, Базы данных и управление данными, Обеспечение качества кода и код ревью.

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**
ПК-9. Способен осуществлять оптимизацию управления жизненным циклом распределенных данных с учетом информационной безопасности	ПК-9.1 Знает методы оптимизации управления жизненным циклом распределенных данных с учетом информационной безопасности	Знать: понятие оптимизации управления жизненным циклом распределенных данных, понятие информационной безопасности Уметь: управлять жизненным циклом распределенных данных, применять методы информационной безопасности Владеть: навыками оптимизации управления жизненным циклом распределенных данных, осуществления информационной безопасности данных

Формируемые и контролируемые компетенции (код и наименование)	**Индикаторы достижения компетенций** (код и наименование)	**Планируемые результаты обучения**
	ПК-9.2 Умеет применять методы оптимизации управления жизненным циклом распределенных данных с учетом информационной безопасности	Знать: методы оптимизации управления жизненным циклом распределенных данных, принципы информационной безопасности Уметь: применять методы оптимизации управления жизненным циклом распределенных данных Владеть: навыками выбора метода оптимизации управления жизненным циклом распределенных данных и их информационной безопасности
	ПК-9.3 Владеет навыками осуществления оптимизации управления жизненным циклом распределенных данных с учетом информационной безопасности	Знать: технологию осуществления оптимизации управления жизненным циклом распределенных данных с учетом информационной безопасности Уметь: проводить оптимизацию управления жизненным циклом распределенных данных с учетом информационной безопасности Владеть: навыками осуществления оптимизации управления жизненным циклом распределенных данных с учетом информационной безопасности

4. Структура и содержание дисциплины Обеспечение безопасности при разработке программного обеспечения

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	лекция	Тема 1. Введение в безопасность при разработке программного обеспечения	4	0,5		-	Собеседование (устный опрос)
	самост. работа	Изучение лекционного материала и подготовка к практическим занятиям	4	10		-	
	лекция	Тема 1.1. Методы оптимизации управления жизненным циклом распределенных данных с учетом информационной безопасности	4	0,5		-	Собеседование (устный опрос)
	самост. работа	Изучение лекционного материала и подготовка к практическим занятиям	4	20		-	
2. Сетевые технологии и информационная безопасность	лекция	Тема 2. Принципы информационной безопасности. Проектирование безопасности	4	0,5		-	Собеседование (устный опрос)
	практ. занятие	План управления жизненным циклом данных для конкретного проекта	4	0,5	20	-	Отчет по практической работе (защита)
	практ. занятие	Анализ и оценка угроз безопасности данных проекта	4	1	20	-	Отчет по практической работе (защита)
	практ. занятие	Проектирование системы защиты данных	4	1	20	-	Отчет по практической работе (защита)
	практ. занятие	Реализация системы защиты данных	4	0,5	20	-	Отчет по практической работе (защита)
	практ. занятие	Тестирование и анализ эффективности примененных мер по обеспечению безопасности данных	4	1	20	-	Отчет по практической работе (защита)
	самост. работа	Изучение лекционного материала и подготовка к практическим занятиям	4	26		-	
	лекция	Тема 3. Технология осуществления оптимизации управления жизненным циклом распределенных данных с учетом информационной безопасности. Разработка безопасности	4	0,5		-	Собеседование (устный опрос)

	самост. работа	Изучение лекционного материала и подготовка к практическим занятиям	4	5		-	
	лекция	Тема 4. Инструменты, используемые для обеспечения безопасности на этапе разработки	4	0,5		-	Собеседование (устный опрос)
	самост. работа	Изучение лекционного материала и подготовка к практическим занятиям	4	10		-	
3. Разработка прикладных задач с учетом требований безопасности	лекция	Тема 5. Оптимизации управления жизненным циклом распределенных данных с учетом информационной безопасности. Обслуживание безопасности	4	0,5		-	Собеседование (устный опрос)
	самост. работа	Изучение лекционного материала и подготовка к практическим занятиям	4	4		-	
	лекция	Тема 6. Угрозы безопасности и методы их предотвращения	4	0,5		-	Собеседование (устный опрос)
	самост. работа	Изучение лекционного материала и подготовка к практическим занятиям	4	10		-	
	лекция	Тема 7. Реагирование на угрозы безопасности	4	0,5		-	Собеседование (устный опрос)
	самост. работа	Изучение лекционного материала и подготовка к практическим занятиям	4	26		-	
	ТИ	Зачет	4		100	-	Итоговый тест по курсу через ОТ
	пром. аттест.	Промежуточная аттестация	4	0,25	0	-	
Итого				108	100		

Схема расчета итогового балла: текущий рейтинг (все занятия и промежуточные тесты) + Результат итогового теста, полученная сумма делится на 2

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 - организация учебного процесса, которая предполагает максимальную активность студентов в процессе формирования ключевых компетенций. На учебной дискуссии студенты представляют результат выполнения заданной работы. Проводится дискуссия по применённым решениям, обсуждается эффективность и архитектура программного кода.

6. Методические указания по освоению дисциплины

6.1 Рекомендации по подготовке к практическим занятиям

Студентам 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 студент 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, студент ликвидирует имеющиеся пробелы в знаниях, углубляет, систематизирует и упорядочивает свои знания. На итоговой сдаче студент демонстрирует то, что он приобрел в процессе обучения по конкретной учебной дисциплине.

Необходимо ориентировать студентов 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
4	ПК-9	Тестовые задания по лекционному материалу. Вопросы к зачету. Отчеты по практическим занятиям.

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 студенту 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 студенту?
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 студенту?
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 материл) последовательности действий проделанных студентом для выполнения заданий. Оформление отчета должно соответствовать методическому указанию рекомендациям, изложенным учебно-методическом пособии [Очеповский А.В. Общие требования по выполнению и оформле-

нию контрольных, курсовых и выпускных квалификационный 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 студентом поставленной цели
6. Обоснованность применяемого решения
7. Грамотность (содержательная) используемых формулировок

Критерии оценки за отчеты по практическим работам:

Полностью выполненное и вовремя защищенный отчет – максимальный балл. За каждое невыполненное задание снимаются баллы в соответствии с заданием на практическое занятие. Просрочка на 1 неделю - коэффициент 0,75, за две - 0,5, за три - 0,25, за четыре и более - 0 (учитывается факт сдачи).

7.3. Оценочные средства для промежуточной аттестации по итогам освоения дисциплины

7.3.1 Вопросы к промежуточной аттестации (зачету)

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?

7.3.2 Критерии и нормы оценки

Семестр	**Форма проведения промежуточной аттестации**[i]	**Критерии и нормы оценки**[ii]	
4	Зачет (по накопительному рейтингу)	зачтено	От 40 до 100 баллов
		незачтено	Менее 40 баллов.

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»

8.2 Дополнительная 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	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

1. Hacking Everything. Режим доступа: http://www.gomzin.com/crypto-gram.html, 2021-01-01.
2. The Tiny Encryption Algorithm (TEA). Режим доступа: http://143.53.36.235:8080/tea.htm, 2021-01-01.
3. Библиотека: Защита информации, криптография. Режим доступа: http://www.win-ni.narod.ru/biblio/cryptobib.htm, 2021-01-01.
4. ДОКТРИНА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙ-СКОЙ ФЕДЕРАЦИИ. Режим доступа: http://www.scrf.gov.ru/documents/5.html, 2021-01-01.
5. Режимы шифрования Олег Зензин. Режим доступа: http://citforum.ru/security/cryptography/rejim_shifrov/, 2021-01-01.
6. Сайт Брюса Шнайера. Schneier on Security. Режим доступа: https://www.schneier.com/, 2021-01-01.
7. Федеральная служба по техническому и экспортному контролю. Режим доступа: http://fstec.ru/, 2021-01-01.

8.4Перечень программного обеспечения

№ п/п	Наименование ПО	Количество лицензий	Реквизиты договора (дата, номер, срок действия)
1	Eclipse Foundation Eclipse версия 4	неограниченный	Лицензия Eclipse Public License
2	NetBeans Community NetBeans IDE версия 8	неограниченный	Лицензия LGPLv2.1, GPLv2 with Classpatch exception
3	The CodeBlocks team CodeBlocks версия 16	неограниченный	Лицензия GNU GPLv3

8.5Описание 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. Помещение для самостоятельной работы. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации. (Г-401)	Столы ученические, стулья ученические, ПК с выходом в сеть Интернет
2	Компьютерный класс. Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для проведения лабораторных работ. Учеб-	Компьютер (монитор 17”, системный блок Intel (R) Celeron (R) 2,66 GHz / 1 Gb / 80 Gb), маршрутиза-

	ная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации. (УЛК-408)	тор 2801 Router, коммутатор Catalyst, экран/интерактивная доска Smart Board TB, проектор Acer P1303W., стол преподавательский, стол ученический, стол компьютерный, стул, доска аудиторная (маркерная).
3	Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации. (УЛК-418)	Стол ученический двухместный (моноблок), доска аудиторная 3-х секционная (меловая), стол преподавательский, стул, проектор Acer

[i] *Указывается форма контроля (зачет, зачет с оценкой, экзамен) и в скобках форма проведения (устно, письменно, по накопительному рейтингу (для дисциплин, реализуемых с БРС)).*

[ii] *Если форма контроля «зачет», то оставить только строки с отметками о зачете, если форма контроля – «зачет с оценкой» или «экзамен», то оставить только строки с оценками.*