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 (специальности)

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

Прикладная информатика в информационной безопасности
(направленность (профиль))

Форма обучения: очная

Год набора: 2023

Общая трудоемкость: **5 ЗЕ**

Распределение часов дисциплины по семестрам

Семестр	**7**	**Итого**
Форма контроля / **Вид занятий**	экзамен	
Лекции	**16**	**16**
Лабораторные		
Практические	**32**	**32**
Руководство: курсовые работы (проекты) / РГР		
Промежуточная аттестация	**0,35**	**0,35**
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» 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» августа 2027 г.

УТВЕРЖДЕНО

На заседании кафедры «Прикладная математика и информатика»
(протокол заседания № 1 от «30» августа 2022 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 1 - Обязательная часть.

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**
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

Формируемые и контролируемые компетенции (код и наименование)	**Индикаторы достижения компетенций** (код и наименование)	**Планируемые результаты обучения**
	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 информационной 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.	Знать: принципы подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом Уметь: составлять обзоры, аннотации, рефераты, научные доклады, публикации, и библиографии по научно-исследовательской работе с учетом Владеть: навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом
ОПК-5. Способен инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных систем	ОПК-5.1. Знает принципы установки программного и аппаратного обеспечения для информационных и автоматизированных систем	Знать: принципы установки программного и аппаратного обеспечения Уметь: применять устанавливать программного и аппаратное обеспечение Владеть: навыками установки программного и аппаратного обеспечения для информационных и автоматизированных систем
	ОПК-5.2. Умеет выполнять настройку информационных и автоматизированных систем	Знать: принципы настройки информационных и автоматизированных систем Уметь: выполнять настройку информационных и автоматизированных систем Владеть: навыками настройки информационных и автоматизированных систем
	ОПК-5.3. Владеет навыками инсталляции программного и аппаратного обеспечения информационных и автоматизированных систем	Знать: программное и аппаратное обеспечение информационных и автоматизированных систем Уметь: инсталлировать программное и аппаратное обеспечение информационных и автоматизированных систем Владеть: навыками инсталлирования программного и аппаратного обеспечения информационных и автоматизированных систем

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. Основы информационной безопасности при разработке программного обеспечения	лекция	Тема 1. Основы информационной безопасности в разработке ПО	7	4		-	Собеседование (устный опрос)
	самост. работа	Изучение лекционного материала и подготовка к практическим занятиям	7	10		-	
	лекция	Тема 1.1. Основные угрозы и уязвимости информационных систем	7	2		-	Собеседование (устный опрос)
	самост. работа	Изучение лекционного материала и подготовка к практическим занятиям	7	10		-	
2. Стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с примене-	лекция	Тема 2. Принципы защиты информации в различных типах информационных систем	7	2		-	Собеседование (устный опрос)
	практ. занятие	План управления жизненным циклом данных для конкретного проекта	7	6	20	-	Отчет по практической работе (защита)
	практ. занятие	Анализ и оценка угроз безопасности данных в информационных и автоматизированных системах	7	8	20	-	Отчет по практической работе (защита)
	практ. занятие	Проектирование системы защиты данных в информационных и автоматизированных системах	7	6	20	-	Отчет по практической работе (защита)
	практ. занятие	Реализация системы защиты данных в информационных и автоматизированных системах	7	6	20	-	Отчет по практической работе (защита)
	практ. занятие	Тестирование и анализ эффективности примененных мер по обеспечению безопасности данных	7	6	20	-	Отчет по практической работе (защита)
	самост. работа	Изучение лекционного материала и подготовка к практическим занятиям	7	17		-	
	лекция	Тема 3. Технология осуществления оптимизации	7	2		-	Собеседование (устный

нием ИКТ и с учетом информационной безопасности		управления жизненным циклом распределенных данных с учетом информационной безопасности. Разработка безопасности					опрос)
	самост. работа	Изучение лекционного материала и подготовка к практическим занятиям	7	5		-	
	лекция	Тема 4. Инструменты, используемые для обеспечения безопасности на этапе разработки	7	1		-	Собеседование (устный опрос)
	самост. работа	Изучение лекционного материала и подготовка к практическим занятиям	7	10		-	
3. Инсталляция программного и аппаратного обеспечения информационных и автоматизированных систем	лекция	Тема 5. Инсталляция программного и аппаратного обеспечения в информационных и автоматизированных системах: методы и инструменты	7	2		-	Собеседование (устный опрос)
	самост. работа	Изучение лекционного материала и подготовка к практическим занятиям	7	5,75		-	
	лекция	Тема 6. Угрозы безопасности и методы их предотвращения	7	2		-	Собеседование (устный опрос)
	самост. работа	Изучение лекционного материала и подготовка к практическим занятиям	7	5		-	
	лекция	Тема 7. Реагирование на угрозы безопасности	7	1		-	Собеседование (устный опрос)
	самост. работа	Изучение лекционного материала и подготовка к практическим занятиям	7	5		-	
	ТИ	Экзамен	7		100	-	Итоговый тест по курсу через ОТ
	пром. аттест.	Промежуточная аттестация	7	0,35	0	-	
Итого				180	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
7	ОПК-3	Тестовые задания по лекционному материалу. Вопросы к зачету. Отчеты по практическим занятиям.
	ОПК-5	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. Основы информационной безопасности при разработке программного обеспечения

1. Что такое информационная безопасность в контексте разработки программного обеспечения?
2. Какие угрозы могут возникнуть при разработке программного обеспечения?
3. Какие виды уязвимостей могут быть обнаружены в программном обеспечении?
4. Какие методы и технологии используются для защиты программного обеспечения от угроз и уязвимостей?
5. Что такое аутентификация и как она используется в программном обеспечении?
6. Как работает шифрование и как оно может быть использовано для защиты программного обеспечения?
7. Какие методы обнаружения и предотвращения взлома могут быть использованы при разработке программного обеспечения?
8. Что такое бэкдор и как он может быть использован для атаки на программное обеспечение?
9. Какие методы и технологии используются для обнаружения и устранения уязвимостей в программном обеспечении?
10. Какие меры безопасности должны быть предприняты при разработке программного обеспечения?
11. Какие риски могут быть связаны с использованием стороннего программного обеспечения?
12. Какие методы и технологии используются для обеспечения конфиденциальности данных в программном обеспечении?
13. Какие методы и технологии используются для обеспечения целостности данных в программном обеспечении?
14. Какие методы и технологии используются для обеспечения доступности данных в программном обеспечении?
15. Какие методы и технологии используются для обнаружения и предотвращения атак на программное обеспечение?

Модуль 2. Стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением ИКТ и с учетом информационной безопасности

1. Какие методы и технологии используются для поиска и анализа информации в Интернете?
2. Какие источники информации являются наиболее надежными и достоверными в современном мире?
3. Какие методы и технологии используются для оформления и подготовки научных статей и публикаций?
4. Какие нормы и правила оформления научных статей и публикаций необходимо соблюдать?
5. Какие методы и технологии используются для оформления и подготовки докладов и презентаций?
6. Какие средства и технологии используются для создания и редактирования документов?
7. Какие методы и технологии используются для организации и управления проектами?
8. Какие методы и технологии используются для обеспечения безопасности при работе с конфиденциальной информацией?
9. Какие методы и технологии используются для обеспечения безопасности при работе с облачными сервисами?
10. Какие методы и технологии используются для обеспечения безопасности при работе с электронной почтой?
11. Какие методы и технологии используются для защиты от кибератак и вирусов?
12. Какие методы и технологии используются для обеспечения конфиденциальности при проведении онлайн-встреч и конференций?
13. Какие методы и технологии используются для обеспечения безопасности при работе с мобильными устройствами?
14. Какие методы и технологии используются для обеспечения безопасности при работе с сетями и Интернетом?
15. Какие методы и технологии используются для обеспечения конфиденциальности при работе с социальными сетями?
16. Какие методы и технологии используются для обеспечения безопасности при работе с банковскими системами и онлайн-платежами?
17. Какие методы и технологии используются для обеспечения безопасности при работе с облачными хранилищами данных?

Модуль 3. Инсталляция программного и аппаратного обеспечения информационных и автоматизированных систем

1. Каковы основные принципы безопасности при разработке программного обеспечения?
2. Какие методы и технологии используются для обеспечения безопасности при разработке программного обеспечения?
3. Какие угрозы могут возникнуть при разработке программного обеспечения и как их можно предотвратить?
4. Какие методы и технологии используются для защиты программного обеспечения от угроз и уязвимостей?
5. Какие методы и технологии используются для обнаружения и предотвращения взлома программного обеспечения?
6. Какие методы и технологии используются для обнаружения и устранения уязвимостей в программном обеспечении?
7. Какие методы и технологии используются для обеспечения защиты данных, хранимых в программном обеспечении?

8. Какие методы и технологии используются для обеспечения безопасности при работе с сторонним программным обеспечением?
9. Какие методы и технологии используются для обеспечения безопасности при работе с облачными сервисами?
10. Какие меры безопасности должны быть предприняты при разработке мобильных приложений?
11. Какие методы и технологии используются для обеспечения безопасности веб-приложений?
12. Какие методы и технологии используются для защиты программного обеспечения от вирусов и кибератак?
13. Какие стандарты и нормы регулируют безопасность при разработке программного обеспечения?
14. Какие меры безопасности необходимо принимать при работе с открытым исходным кодом?
15. Какие методы и технологии используются для оценки безопасности программного обеспечения?
16. Какие меры безопасности необходимо принимать при тестировании программного обеспечения?
17. Каковы последствия небезопасного программного обеспечения и как их можно предотвратить?

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 в информационных и автоматизированных системах»

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 в информационных и автоматизированных системах»

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 в информационных и автоматизированных системах»

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 оформлению 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 (экзамену)

1. Что такое обеспечение безопасности при разработке программного обеспечения?
2. Какие принципы обеспечения безопасности необходимо учитывать при разработке программного обеспечения?
3. Какие методы и средства используются для обеспечения безопасности при разработке программного обеспечения?
4. Какие требования к информационной безопасности необходимо учитывать при разработке программного обеспечения?
5. Что такое информационно-коммуникационные технологии и как они связаны с обеспечением безопасности при разработке ПО?
6. Какие стандарты регулируют обеспечение безопасности при разработке программного обеспечения?
7. Какие угрозы безопасности могут возникнуть при разработке программного обеспечения?
8. Какие виды атак могут быть проведены на программное обеспечение и как их предотвратить?
9. Какие методы аутентификации и авторизации могут быть использованы для обеспечения безопасности программного обеспечения?
10. Какие методы шифрования могут быть использованы для защиты данных в программном обеспечении?
11. Какие методы обнаружения и предотвращения вредоносных программ могут быть использованы при разработке ПО?
12. Какие методы обнаружения и предотвращения атак на программное обеспечение могут быть использованы при разработке ПО?
13. Какие методы обеспечения безопасности сетей могут быть использованы при разработке ПО?

14. Какие методы обеспечения безопасности баз данных могут быть использованы при разработке ПО?

15. Какие методы обеспечения безопасности веб-приложений могут быть использованы при разработке ПО?

16. Какие методы обеспечения безопасности мобильных приложений могут быть использованы при разработке ПО?

17. Какие методы обеспечения безопасности встроенных систем могут быть использованы при разработке ПО?

18. Какие методы тестирования безопасности программного обеспечения могут быть использованы при разработке ПО?

19. Какие методы обеспечения безопасности при работе с облачными сервисами могут быть использованы при разработке ПО?

20. Какие методы обеспечения безопасности при работе с микросервисами могут быть использованы при разработке ПО?

21. Какие методы обеспечения безопасности при работе с контейнерами могут быть использованы при разработке ПО?

22. Какие методы обеспечения безопасности при работе с открытым исходным кодом могут быть использованы при разработке ПО?

23. Какие методы обеспечения безопасности при работе с командами разработчиков могут быть использованы при разработке ПО?

24. Какие методы обеспечения безопасности при работе с третьими сторонами могут быть использованы при разработке ПО?

25. Какие методы управления доступом могут быть использованы для обеспечения безопасности программного обеспечения?

26. Какие методы мониторинга безопасности могут быть использованы для обеспечения безопасности программного обеспечения?

27. Какие методы резервного копирования могут быть использованы для обеспечения безопасности программного обеспечения?

28. Какие методы обеспечения безопасности при установке и конфигурации программного обеспечения могут быть использованы при разработке ПО?

29. Какие методы обеспечения безопасности при обновлении программного обеспечения могут быть использованы при разработке ПО?

30. Какие методы обеспечения безопасности при эксплуатации программного обеспечения могут быть использованы при разработке ПО?

31. Какие методы обеспечения безопасности при удалении программного обеспечения могут быть использованы при разработке ПО?

32. Какие методы обеспечения безопасности при передаче данных между приложениями могут быть использованы при разработке ПО?

33. Какие методы обеспечения безопасности при работе с различными операционными системами могут быть использованы при разработке ПО?

34. Какие методы обеспечения безопасности при работе с различными браузерами могут быть использованы при разработке ПО?

35. Какие методы обеспечения безопасности при работе с различными языками программирования могут быть использованы при разработке ПО?

36. Какие методы обеспечения безопасности при работе с различными протоколами связи могут быть использованы при разработке ПО?

37. Какие методы обеспечения безопасности при работе с различными форматами данных могут быть использованы при разработке ПО?

38. Какие методы обеспечения безопасности при работе с различными устройствами могут быть использованы при разработке ПО?

39. Какие методы обеспечения безопасности при работе с различными средами разработки могут быть использованы при разработке ПО?

40. Какие методы обеспечения безопасности при работе с различными инструментами разработки могут быть использованы при разработке ПО?

41. Какие методы обеспечения безопасности при работе с различными фреймворками и библиотеками могут быть использованы при разработке ПО?

42. Какие методы обеспечения безопасности при работе с различными модулями и компонентами могут быть использованы при разработке ПО?

43. Какие методы обеспечения безопасности при работе с различными сервисами могут быть использованы при разработке ПО?

44. Какие методы обеспечения безопасности при работе с различными протоколами и стандартами могут быть использованы при разработке ПО?

45. Какие методы обеспечения безопасности при работе с различными операционными средами могут быть использованы при разработке ПО?

46. Какие методы обеспечения безопасности при работе с различными типами угроз могут быть использованы при разработке ПО?

47. Какие методы обеспечения безопасности при работе с различными типами данных могут быть использованы при разработке ПО?

48. Какие методы обеспечения безопасности при работе с различными типами пользователей могут быть использованы при разработке ПО?

49. Какие методы обеспечения безопасности при работе с различными типами устройств могут быть использованы при разработке ПО?

50. Какие методы обеспечения безопасности при работе с различными типами сетей могут быть использованы при разработке ПО?

51. Какие методы обеспечения безопасности при работе с различными типами архитектур могут быть использованы при разработке ПО?

52. Какие методы обеспечения безопасности при работе с различными типами приложений могут быть использованы при разработке ПО?

53. Какие методы обеспечения безопасности при работе с различными типами сервисов могут быть использованы при разработке ПО?

54. Какие методы обеспечения безопасности при работе с различными типами баз данных могут быть использованы при разработке ПО?

55. Какие методы обеспечения безопасности при работе с различными типами уязвимостей могут быть использованы при разработке ПО?

56. Какие методы обеспечения безопасности при работе с различными типами атак могут быть использованы при разработке ПО?

57. Какие методы обеспечения безопасности при работе с различными типами устройств хранения данных могут быть использованы при разработке ПО?

58. Какие методы обеспечения безопасности при работе с различными типами протоколов и форматов данных могут быть использованы при разработке ПО?

59. Какие методы обеспечения безопасности при работе с различными типами аутентификации и авторизации могут быть использованы при разработке ПО?

60. Какие методы обеспечения безопасности при работе с различными типами шифрования могут быть использованы при разработке ПО?

61. Какие методы обеспечения безопасности при работе с различными типами облачных сервисов могут быть использованы при разработке ПО?

62. Какие методы обеспечения безопасности при работе с различными типами мобильных устройств могут быть использованы при разработке ПО?

63. Какие методы обеспечения безопасности при работе с различными типами операционных систем могут быть использованы при разработке ПО?

64. Какие методы обеспечения безопасности при работе с различными типами протоколов передачи данных могут быть использованы при разработке ПО?

65. Какие методы обеспечения безопасности при работе с различными типами браузеров могут быть использованы при разработке ПО?

66. Какие методы обеспечения безопасности при работе с различными типами скриптовых языков могут быть использованы при разработке ПО?

67. Какие методы обеспечения безопасности при работе с различными типами интеграций могут быть использованы при разработке ПО?

68. Какие методы обеспечения безопасности при работе с различными типами аппаратных средств могут быть использованы при разработке ПО?

69. Какие методы обеспечения безопасности при работе с различными типами вебсерверов могут быть использованы при разработке ПО?

70. Какие методы обеспечения безопасности при работе с различными типами клиентских приложений могут быть использованы при разработке ПО?

71. Какие методы обеспечения безопасности при работе с различными типами серверных приложений могут быть использованы при разработке ПО?

72. Какие методы обеспечения безопасности при работе с различными типами протоколов удаленного доступа могут быть использованы при разработке ПО?

73. Какие методы обеспечения безопасности при работе с различными типами систем управления базами данных могут быть использованы при разработке ПО?

74. Какие методы обеспечения безопасности при работе с различными типами средств разработки могут быть использованы при разработке ПО?

75. Какие методы обеспечения безопасности при работе с различными типами средств автоматизации тестирования могут быть использованы при разработке ПО?

76. Какие методы обеспечения безопасности при работе с различными типами систем контроля версий могут быть использованы при разработке ПО?

77. Какие методы обеспечения безопасности при работе с различными типами архивных форматов могут быть использованы при разработке ПО?

78. Какие методы обеспечения безопасности при работе с различными типами систем мониторинга и анализа могут быть использованы при разработке ПО?

79. Какие методы обеспечения безопасности при работе с различными типами программных интерфейсов могут быть использованы при разработке ПО?

80. Какие методы обеспечения безопасности при работе с различными типами архитектурных шаблонов могут быть использованы при разработке ПО?

81. Какие методы обеспечения безопасности при работе с различными типами виртуализации могут быть использованы при разработке ПО?

82. Какие методы обеспечения безопасности при работе с различными типами распределенных систем могут быть использованы при разработке ПО?

83. Какие методы обеспечения безопасности при работе с различными типами нейронных сетей и машинного обучения могут быть использованы при разработке ПО?

84. Какие методы обеспечения безопасности при работе с различными типами систем автоматизации бизнес-процессов могут быть использованы при разработке ПО?

85. Какие методы обеспечения безопасности при работе с различными типами систем управления проектами могут быть использованы при разработке ПО?

86. Какие методы обеспечения безопасности при работе с различными типами систем управления версиями документов могут быть использованы при разработке ПО?

87. Какие методы обеспечения безопасности при работе с различными типами систем управления контентом могут быть использованы при разработке ПО?

88. Какие методы обеспечения безопасности при работе с различными типами систем управления производственными процессами могут быть использованы при разработке ПО?

89. Какие методы обеспечения безопасности при работе с различными типами систем управления складскими процессами могут быть использованы при разработке ПО?

90. Какие методы обеспечения безопасности при работе с различными типами систем управления логистическими процессами могут быть использованы при разработке ПО?

7.3.2 Критерии и нормы оценки

Семестр	Форма проведения промежуточной аттестации[i]	Критерии и нормы оценки[ii]	
7	Экзамен (по накопительному рейтингу)	отлично	от 85 до 100 баллов
		хорошо	от 70 до 84 баллов
		удовлетворительно	от 55 до 69 баллов
		неудовлетворительно	от 0 до 54 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.*