

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

09.03.03 Прикладная информатика

Разработка программного обеспечения

Форма обучения: очная

Год набора: 2023

Общая трудоемкость: **5 ЗЕ**

Распределение часов дисциплины по семестрам

Семестр	<u>7</u>	Итого
Вид занятий Форма контроля	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(и):

доцент кафедры «Прикладная математика и информатика» доцент к.т.н. Кузьмичев А.Б.

(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 31.08.2027 г.

УТВЕРЖДЕНО

На заседании кафедры «Прикладная математика и информатика»
(протокол заседания № 1 от « 30 » августа 2022 г.).

1. Цель освоения дисциплины

Цель – изучение основных понятий, методов и средств защиты информации в процессе ее обработки, передачи и хранения в современных информационных технологиях и системах.

Задачи:

1. Дать основные понятия и определения в области защиты информации.
2. Дать источники угроз и форм атак на компьютерную информацию, направления защиты информации от всевозможных угроз.
3. Дать и получить навыки по разработке простейших криптографических систем.
4. Дать и получить навыки по разработке политики информационной безопасности.
5. Дать базовые технологии защиты информации.

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

Данная дисциплина (учебный курс) относится к Б1 "Дисциплины (модули)" (Обязательная часть).

Дисциплины, учебные курсы, на освоении которых базируется данная дисциплина (учебный курс) – .

Дисциплины, учебные курсы, для которых необходимы знания, умения, навыки, приобретаемые в результате изучения данной дисциплины (учебного курса) – .

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.	<p>Знать: стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности</p> <p>Уметь: применять стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности</p> <p>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</p>
	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>
ОПК -5. Способен устанавливать программное и аппаратное обеспечение для информационных и автоматизированных систем;	ОПК-5.1. Знает принципы установки программного и аппаратного обеспечения для информационных и автоматизированных систем	<p>Знать: принципы установки программного и аппаратного обеспечения</p> <p>Уметь: применять устанавливать программного и аппаратное обеспечение</p> <p>Владеть: навыками установки программного и аппаратного обеспечения для информационных и автоматизированных систем</p>
	<p>ОПК-5.2. Умеет выполнять настройку информационных и автоматизированных систем</p> <p>ОПК-5.3. Владеет навыками инсталляции программного и аппаратного обеспечения информационных и автоматизированных систем</p>	<p>Знать: принципы настройки информационных и автоматизированных систем</p> <p>Уметь: выполнять настройку информационных и автоматизированных систем</p>

	тизированных систем	<p>стем Владеть: навыками настройки информационных и автоматизированных систем</p> <p>Знать: программное и аппаратное обеспечение информационных и автоматизированных систем</p> <p>Уметь: устанавливать программное и аппаратное обеспечение информационных и автоматизированных систем</p> <p>Владеть: навыками installations программного и аппаратного обеспечения информационных и автоматизированных систем</p>
--	---------------------	---

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	лекция	Тема 1.1.Основные понятия и определения безопасности информации. Классификация угроз безопасности информации	7	2		-	Собеседование (устный опрос)
	самост. работа	Изучение лекционного материала и подготовка к практическим занятиям	7	16		-	
	лекция	Тема 1.2.Классификация методов противодействия угрозам безопасности информации	7	2		-	Собеседование (устный опрос)
	самост. работа	Изучение лекционного материала и подготовка к практическим занятиям	7	16		-	
2.Криптографические методы защиты информации	лекция	Тема 2.1.Основы симметричных алгоритмов и криптосистем	7	2		-	Собеседование (устный опрос)
	практ. занятие	Разработка программы по реализации блочно-го симметричного алгоритма шифрования	7	6		-	Отчет по практической работе (защита)
	практ. занятие	Разработка программы шифрования и де-шифрирования произвольного файла по алгоритму создания цепочек OFB	7	6		-	Отчет по практической работе (защита)
	практ. занятие	Разработка программы реализации алгоритма хеширования для создания ключа на основе пароля	7	4		-	Отчет по практической работе (защита)
	практ. занятие	Разработка подсистемы шифрования для симметричной криптосистемы	7	4		-	Отчет по практической работе (защита)
	практ. занятие	Разработка программы, реализующую симметричную криптосистему	7	4		-	Отчет по практической работе (защита)
	самост. работа	Изучение лекционного материала и подготовка к практическим занятиям	7	24		-	

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
	лекция	Тема 2.2.Асимметричные криптоалгоритмы и крипто-системы	7	1		-	Собеседование (устный опрос)
	практ. занятие	Разработка программы сжатия данных с целью уменьшения энтропии информации по алгоритму RLE или LZW	7	4		-	Отчет по практической работе (защита)
	самост. работа	Изучение лекционного материала и подготовка к практическим занятиям	7	12		-	
	лекция	Тема 2.3.Электронная цифровая подпись	7	1		-	Собеседование (устный опрос)
	самост. работа	Изучение лекционного материала и подготовка к практическим занятиям	7	12		-	
3.Базовые технологии защиты информации в информационных технологиях	лекция	Тема 3.1.Основные понятия идентификации и аутентификации	7	2		-	Собеседование (устный опрос)
	самост. работа	Изучение лекционного материала и подготовка к практическим занятиям	7	2		-	
	лекция	Тема 3.2.Модели безопасности информационных систем	7	1		-	Собеседование (устный опрос)
	самост. работа	Изучение лекционного материала и подготовка к практическим занятиям	7	2		-	
4.Политика информационной безопасности	лекция	Тема 4.1.Стандарты информационной безопасности	7	1		-	Собеседование (устный опрос)
	самост. работа	Изучение лекционного материала и подготовка к практическим занятиям	7	2		-	
	лекция	Тема 4.2.Расчет рисков в области информационной безопасности	7	2		-	Собеседование (устный опрос)

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
	самост. работа	Изучение лекционного материала и подготовка к практическим занятиям	7	2		-	
	лекция	Тема 4.3. Основы разработки политики информационной безопасности	7	2		-	Собеседование (устный опрос)
	практ. занятие	Разработка политики информационной безопасности организации 1	7	2		-	Отчет по практической работе (защита)
	практ. занятие	Разработка политики информационной безопасности организации 2	7	4		-	Отчет по практической работе (защита)
	самост. работа	Изучение лекционного материала и подготовка к практическим занятиям	7	8		-	
	ТИ	Экзамен	7			-	Итоговый тест по курсу через ОТ
	пром. аттест.	Промежуточная аттестация	7			-	
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 - 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 по сдаче дисциплины. Отчеты по практическим занятиям.
7	ОПК-5	Тестовые задания по лекционному материалу. Вопросы по сдаче дисциплины. 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

1. Перечислите свойства информации.
2. Назовите предмет и объект защиты информации.
3. Что такое безопасность информации в компьютерных системах?
4. Что такое система защиты информации?
5. Что такое угроза безопасности информации?
6. Что такое конфиденциальность информации?
7. Что такое целостность информации?
8. Что такое доступность информации?
9. Перечислите случайные угрозы безопасности информации.
10. Что такое нарушитель информации и злоумышленник?
11. Перечислите преднамеренные угрозы безопасности информации.

Модуль 2. Криптографические методы защиты информации

1. Что такое криптография, криптоанализ и криптология?
2. Что такое криптосистема?
3. Перечислите и охарактеризуйте методы криптографических преобразований.
4. Дайте классификацию криптоалгоритмов.
5. Дайте понятие основных операций, используемых в алгоритмах шифрования.
6. Дайте понятие потокового и блочного шифра.
7. Перечислите операции, используемые в алгоритмах блочных шифров.
8. Приведите схему шифрования и дешифрирования по сети Фейстеля.
9. ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.
10. Что такое режимы шифрования?
11. Раскройте принцип реализации режима шифрования обратная связь по выходу (OFB).
12. Раскройте принципы внесения случайности в сообщения при шифровании.
13. Приведите способы генерации случайных чисел.

14. Понятие и свойства Хеш-функции.
15. Приведите пример алгоритма приведения пароля пользователя к заданной длине ключа с помощью Хеш-функции.
16. Приведите общую схему симметричной криптосистемы.
17. Основная идея асимметричных криптоалгоритмов?
18. Приведите необходимые условия реализации асимметричной криптографии.
19. Приведите примеры асимметричных криптоалгоритмов.
20. Общая схема асимметричной криптосистемы.
21. Первый этап алгоритма RSA по созданию пары ключей.
22. Этап передачи зашифрованного сообщения в алгоритме RSA.
23. Понятие и свойства Хеш-функции.
24. Приведите примеры использования и реализаций криптографических Хеш-функций.
25. Раскройте алгоритм Меркеля-Дамгарда по реализации хеш-функции.
26. Алгоритм вычисления хеш-функции согласно ГОСТ Р 34.11-2012.
27. Схема алгоритма Девиса и Майера для хеширования паролей.
28. Назначение и виды защиты от злоумышленных действий при использовании ЭЦП.
29. Алгоритм формирования и проверки ЭЦП.
30. Алгоритм формирования ЭЦП по ГОСТ Р 34.10-2012.

Модуль 3. Базовые технологии защиты информации в информационных технологиях

1. Перечислите и дайте понятия базовых технологий защиты информации.
2. Дайте классификацию процессов аутентификации.
3. В чем заключается строгая аутентификация.
4. В чем заключается простая аутентификация.
5. Основы биометрической аутентификации.
6. Что такое Хеширование пароля?
7. Дайте характеристики криптографических хеш-функций.
8. Дайте характеристики методов простой и биометрической аутентификации.
9. Приведите алгоритм строгой аутентификации на основе симметричных алгоритмов.
10. Что такое Модель политики информационной безопасности?
11. Приведите классы модели политики информационной безопасности.
12. Раскройте дискреционную модель Харрисона-Рузо-Ульмана.
13. Что такое матричное разграничение доступа. Приведите пример реализации.
14. Что такое мандатное разграничение доступа. Приведите пример реализации.

Модуль 4. Политика информационной безопасности

1. Контрольные функции в области государственной безопасности, возложенные на ФСТЭК России?
2. Основные законы Российской Федерации, связанные с защитой информации.
3. Указы Президента, связанные с защитой информации.
4. Приказы ФСТЭК России, связанные с защитой информации.
5. Методические и руководящие документы ФСТЭК, связанные с защитой информации.
6. Статья Кодекса Административных правонарушений, Гражданского и Уголовного кодекса
7. 7 уровней безопасности, определенные в Оранжевой книге.
8. 6 базовых требований безопасности, определенные в Оранжевой книге.
9. 10 классов безопасности информации, установленные в европейских стандартах.
10. Перечислите основные пути получения информации о системе защиты?
11. Дайте классификацию информационных объектов по требуемой степени безотказности.

12. Дайте классификацию информационных объектов по уровню конфиденциальности.
13. Что такое риск информационной безопасности и как он вычисляется.
14. Перечислите уровни ущерба от реализации рисков.
15. Приведите пример формирования оценки вероятности атак на информацию.
16. Дайте алгоритм расчета риска информационной безопасности.
17. Что такое политика информационной безопасности?
18. Перечислите требования к системе безопасности.
19. Раскройте принципа доступа к информационным ресурсам организации.
20. Опишите основные направления разработки политики безопасности.
21. Перечислите этапы разработки политики информационной безопасности

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 «Разработка программы по реализации блочно-го симметричного алгоритма шифрова-ния»

Форма отчета по практическому занятию №1

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

Практическое занятие №2 «Разработка программы шифрования и де-шиффрирова-ния произ-вольного файла по алгоритму создания цепочек OFB»

Форма отчета по практическому занятию №2

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

Практическое занятие №3 «Разработка программы реализации алгоритма хеши-рования для создания ключа на основе пароля»

Форма отчета по практическому занятию №3

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

Практическое занятие №4 «Разработка подсистемы шифрования для симметрич-ной крип-тосистемы»

Форма отчета по практическому занятию №4

- титульный лист;

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

Практическое занятие №5 «Разработка программы, реализующую симметричную криптосистему»

Форма отчета по практическому занятию №5

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

Практическое занятие №6 «Разработка программы сжатия данных с целью уменьшения энтропии информации по алгоритму RLE или LZW»

Форма отчета по практическому занятию №6

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

Практическое занятие №7 «Разработка политики информационной безопасности организации 1»

Форма отчета по практическому занятию №7

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

Практическое занятие №8 «Разработка политики информационной безопасности организации 2»

Форма отчета по практическому занятию №8

- 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 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 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 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

1. Основные понятия и определения безопасности информации.
2. Классификация угроз безопасности информации
3. Классификация методов противодействия угрозам безопасности информации.
4. Правовые методы защиты информации
5. Методы защиты информации от случайных угроз.
6. Методы защиты информации от шпионажа и диверсий.
7. Методы защиты информации от электромагнитных излучений и наводок.
8. Методы защиты информации от несанкционированного доступа.
9. Концепции построения систем разграничения доступа.
10. Криптографические методы защиты
11. Основы симметричных криптоалгоритмов.
12. Криптоалгоритм на основе сети Файстеля.
13. Блочный шифр DES
14. Алгоритмы создания цепочек.
15. Методы рандомизации сообщений.
16. Классификация алгоритмов архивации данных
17. Хеш-функция и её реализация
18. Функции симметричной криптосистемы
19. Обобщенная схема симметричной криптосистемы
20. Асимметричные криптоалгоритмы
21. Асимметричный алгоритм шифрования RSA.
22. Электронная цифровая подпись
23. Основные понятия идентификации и аутентификации
24. Простая аутентификация
25. Методы строгой аутентификации.
26. Стандарты информационной безопасности.
27. Базовые технологии защиты информации в вычислительных сетях.
28. Модели безопасности операционных систем
29. Классификация информационных объектов по категориям информационной безопасности
30. Требования к системам защиты информации.
31. Порядок разработки политики информационной безопасности.
32. Многоуровневая защита систем обработки информации.
33. Методы защиты информации от несанкционированного изменения структуры систем
34. Источники атак на информацию
35. Риски в использовании информации
36. Формы атак на информацию
37. Организационные методы защиты информации.

38. Блочный шифр ГОСТ 28147-89
39. Алгоритмы архивации Хаффмана.
40. Алгоритмы архивации Лемпеля-Зива
41. Алгоритмы архивации RLE
42. Транспортное кодирование.
43. Классификация алгоритмов хэширования
44. Хеширование паролей.
45. Общая схема симметричной криптосистемы
46. Общая схема асимметричной криптосистемы.
47. Алгоритм вычисления хеш-функции согласно ГОСТ Р 34.11-2012
48. ЭЦП с дополнительными свойствами.
49. Классификация процессов аутентификации.
50. Основы биометрической аутентификации и идентификации
51. Основы администрирования вычислительных сетей
52. Расчет рисков информационной безопасности
53. Методы внесения случайности в сообщения
54. Асимметричный алгоритм шифрования RSA
55. Основная законодательная база в области информационных технологий
56. Международные стандарты информационной безопасности
57. Основы хеширования и хранения паролей
58. Дискреционная модель Харрисона-Рузо-Ульмана
59. Реализация системы разграничения доступа в операционных системах
60. Основные пути получения информации о системе защиты информации
61. Понятие политики информационной безопасности
62. Классификация режимов шифрования
63. Режим шифрования ECB
64. Режим шифрования OFB
65. Режим шифрования CFB
66. Режим шифрования CBC
67. Требования защищенности средств вычислительной техники от несанкционированного доступа к информации
68. Алгоритм Меркеля-Дамгарда по реализации хеш-функции
69. Алгоритм формирования ЭЦП по ГОСТ Р 34.10-2012
70. Операции, используемые в алгоритмах блочных шифров

7.3.2 Критерии и нормы оценки

Семестр	Форма проведения промежуточной аттестации	Критерии и нормы оценки	
7	Экзамен (по накопительному рейтингу)	отлично	если даны правильные и четкие ответы на вопросы, правильные и четкие ответы на дополнительные вопросы, продемонстрирована способность формировать и обоснованно отстаивать собственное мнение;
		хорошо	если даны правильные, но не всегда полные ответы на вопросы, дополнительные вопросы;

Семестр	Форма проведения промежуточной аттестации	Критерии и нормы оценки	
			возникают трудности в формировании обоснованного собственного мнения;
		удовлетворительно	если даны правильные, но не полные ответы на вопросы, возникают проблемы при ответе на дополнительные вопросы, проблемы при формировании собственного мнения;
		неудовлетворительно	если ответы на основные вопросы даны в объеме менее 50%, ответы на дополнительные вопросы вызывают большие затруднения (практически не верны).

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-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

1. Hacking Everything. Режим доступа: <http://www.gomzin.com/crypto-gram.html>, 2022-01-01.
2. The Tiny Encryption Algorithm (TEA). Режим доступа: <http://143.53.36.235:8080/tea.htm>, 2022-01-01.
3. Библиотека: Защита информации, криптография. Режим доступа: <http://www.win-ni.narod.ru/biblio/cryptobib.htm>, 2022-01-01.
4. ДОКТРИНА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ. Режим доступа: <http://www.scrf.gov.ru/documents/5.html>, 2022-01-01.
5. Режимы шифрования Олег Зензин. Режим доступа: http://citforum.ru/security/cryptography/rejim_shifrov/, 2022-01-01.
6. Сайт Брюса Шнайера. Schneier on Security. Режим доступа: <https://www.schneier.com/>, 2022-01-01.
7. Федеральная служба по техническому и экспортному контролю. Режим доступа: <http://fstec.ru/>, 2022-01-01.

8.4 Перечень 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	Microsoft Office Standard версия 2007	636	
3	NetBeans Community NetBeans IDE версия 8	неограниченный	Лицензия LGPLv2.1, GPLv2 with Classpatch exception
4	The CodeBlocks team CodeBlocks версия 16	неограниченный	Лицензия GNU GPLv3

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. 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	Компьютер (монитор 19", системный блок Pentium (R) Dual-Core E5500 2,8

	<p>аудитория для проведения лабораторных работ. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций</p> <p>Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации. (УЛК-401)</p>	<p>GHz / 4 Gb / 500 Gb) , стол ученический, стол компьютерный, стол преподавательский, стулья, Доска аудиторная(меловая).</p>
3	<p>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 проведения групповых и индивидуальных консультаций</p> <p>Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации. (УЛК-408)</p>	<p>Компьютер (монитор 17", системный блок Intel (R) Celeron (R) 2,66 GHz / 1 Gb / 80 Gb), маршрутизатор 2801 Router, коммутатор Catalyst, экран/интерактивная доска Smart Board TV, проектор Acer P1303W., стол преподавательский, стол ученический, стол компьютерный, стул, доска аудиторная (маркерная).</p>
4	<p>Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ).</p> <p>Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации. (УЛК-418)</p>	<p>Стол ученический двухместный (моноблок), доска аудиторная 3-х секционная (меловая), стол преподавательский, стул, проектор Acer</p>