федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

_Б1.В.ДВ.01.01_
(индекс дисциплины)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Безопасность корпоративных информационных систем

(наименование дисциплины)

по направлению подготовки (специальности)
09.04.03 Прикладная информатика

(кол и наименование направления подготовки, специальность в соответствии с ФГОС ВПО/ФГОС ВО)

Информационные системы и технологии корпоративного управления

(направленность, профиль)

Форма обучения: _очная_
Год набора: _2019_

Распределение часов дисциплины по семестрам и видам занятий (по учебному плану)

Количество ЗЕТ	7											
Часов по РУП	252											
Виды контроля в семестрах:	**Экзамены**		**Зачеты**			**Курсовые проекты**		**Курсовые работы**			**Контрольные работы (для заочной ф/о)**	
			3									
	№№ семестров											
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**Итого**
ЗЕТ по семестрам			7									7
Лекции			34									34
Лабораторные			8									8
Практические			50									50
Промежуточная аттестация			0,25									0,25
Контактная работа			92,25									92,25
Сам. работа			160									160
Контроль												
Итого			252									252

Тольятти, 2019

Рабочая программа составлена на основании ФГОС ВО и учебного плана направления подготовки _09.04.03 Прикладная информатика_

(код и наименование направления подготовки в соответствии с ФГОС ВО)

Рецензирование рабочей программы дисциплины:

☒ Отсутствует

☒ Учебная (рабочая) программа одобрена на заседании кафедры _____ (протокол заседания № 6 от "13" февраля 2019 г.).

☐ Рецензент

_____ _____ _____

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

«___»_____20___г.

Срок действия рабочей программы дисциплины до « 31 » августа 2021 г.

Информация об актуализации рабочей программы дисциплины:

Протокол заседания кафедры № 1 от «09» сентября 2019 г.

Протокол заседания кафедры № 1 от « 28» августа 2020 г.

Протокол заседания кафедры № ___от «__»_____ 20__ г.

Протокол заседания кафедры № ___от «__»_____ 20__ г.

УТВЕРЖДАЮ

Заведующий кафедрой Прикладная математика и информатика

(разработавшей РПД)

« » 20 г. _____ А.В. Очеповский

(подпись) *(И.О. Фамилия)*

АННОТАЦИЯ
дисциплины (учебного курса)
Б1.В.ДВ.01.01 Безопасность корпоративных информационных систем

(индекс и наименование дисциплины (учебного курса))

1. Цель и задачи изучения дисциплины (учебного курса)

Цель – развитие у обучающихся знаний и получении навыков по разработке и реализации защиты информации на основе современных методов криптографии в области построения и эксплуатации корпоративных информационных систем

Задачи:

1. Сформировать у обучающихся продвинутые знания в области криптографических методов защиты информации
2. Развить у обучающихся практические навыки в области проектирования и реализации криптосистем
3. Выработать у обучающихся способность разрабатывать политику информационной безопасности с заданным уровнем защиты информации

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

Данная дисциплина (учебный курс) относится к Дисциплины по выбору.

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

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

3. Планируемые результаты обучения по дисциплине (учебному курсу), соотнесенные с планируемыми результатами освоения образовательной программы

Формируемые и контролируемые компетенции	Планируемые результаты обучения
ПК-4: Способен управлять информационными ресурсами и ИС	знать: Основные руководящие документы по реализации защиты информации, применительно к корпоративной информационной системе знать: Основы проведения политики безопасности знать: Основы Хэш-функций знать: Базовые технологии защиты информации: идентификация и аутентификация, авторизация, аудит и шифрование уметь: Разрабатывать криптографическую систему на основе российских стандартов владеть: Навыками разработки системы реализации электронной цифровой подписи владеть: Навыками разработки политики безопасности при внедрении и эксплуатации корпоративной информационной системы
ПК-5: Способен управлять проектами по информатизации прикладных задач и созданию ИС предприятий и организаций	знать: Российские стандарты для криптографической защиты информации, применительно к корпоративной информационной системы знать: Криптографические алгоритмы шифрования знать: Основы реализации электронной цифровой подписи уметь: Проводить анализ степени защиты корпоративной информационной

	системы методом сверху -вниз уметь: Разрабатывать систему реализации электронной цифровой подписи владеть: Навыками разработки криптографической системы на основе современной среды программирования, применительно к корпоративной информационной системе

Тематическое содержание дисциплины (учебного курса)

Раздел, модуль	Подраздел, тема
Модуль 1. Криптографические алгоритмы защиты информации в корпоративных информационных системах	Тема 1. Симметричная криптографическая система Тема 2. Асимметричная криптографическая система
Модуль 2. Стандарты информационной безопасности и модели безопасности информационных систем	Тема 3. Стандарты информационной безопасности Тема 4. Базовые технологии защиты информации в вычислительных сетях Тема 5. Модели безопасности информационных систем
Модуль 3. Политика информационной безопасности	Тема 6. Анализ безопасности информации в корпоративной ин-формационной системе Тема 7. Основы разработки политики информационной безопасности

Общая трудоемкость дисциплины (учебного курса) – _7_ ЗЕТ.

4. Структура и содержание дисциплины (учебного курса) Безопасность корпоративных информационных систем

Семестр изучения 3

Раздел, модуль	Подраздел, тема	Виды учебной работы							Необходимые материально-технические ресурсы	Формы текущего контроля (наименование оценочного средства)	Рекомендуемая литература (№)
		Контактная работа (в часах)					Самостоятельная работа				
		всего			в т.ч. в интерактивной форме	Формы проведения лекций, лабораторных, практических занятий, методы обучения, реализующие применяемую образовательную технологию	в часах	формы организации самостоятельной работы			
		лекций	лабораторных	практических							
Криптографические алгоритмы защиты информации в корпоративных информационных системах	Симметричная криптографическая система	8				Лекция		Работа с лекционным материалом и учебной литературой	Класс с медиаоборудованием	Собеседование (устный опрос)	1-3
	Разработка программы по реализации блочного симметричного алгоритма шифрования			10	10	Компьютерный практикум		Подготовка к практическим занятиям и отчета по работе	Лаборатория с компьютерами	Отчет по практической работе (защита)	1-3
	Разработка программы шифрования и дешифрирования произвольного файла по алгоритму создания цепочек OFB			8	8	Компьютерный практикум		Подготовка к практическим занятиям и отчета по работе	Лаборатория с компьютерами	Отчет по практической работе (защита)	1-3
	Разработка программы реализации алгоритма хеширования для создания ключа на основе пароля			8	8	Компьютерный практикум		Подготовка к практическим занятиям и отчета по работе	Лаборатория с компьютерами	Отчет по практической работе (защита)	1-3
	Разработка подсистемы шифрования для симметричной криптосистемы			8	8	Компьютерный практикум		Подготовка к практическим занятиям и отчета по работе	Лаборатория с компьютерами	Отчет по практической работе (защита)	1-3
	Разработка подсистемы дешифрирования для симметричной криптосистемы			8	8	Компьютерный практикум	26	Подготовка к практическим занятиям и отчета по работе	Лаборатория с компьютерами	Отчет по практической работе (защита)	1-3
	Асимметричная криптографическая система	4				Лекция		Работа с лекционным материалом и учебной	Класс с медиаоборудованием	Собеседование (уст-	1-3

								литературой		ный опрос)	
	Разработка программы сжатия данных с целью уменьшения энтропии информации по алгоритму RLE или LZW		4		4	Компьютерный практикум	28	Подготовка к практическим занятиям и отчета по работе	Лаборатория с компьютерами	Отчет по практической работе	1-3
Стандарты информационной безопасности и модели безопасности информационных систем	Стандарты информационной безопасности	6				Лекция	20	Работа с лекционным материалом и учебной литературой	Класс с медиаоборудованием	Собеседование (устный опрос)	1-3
	Базовые технологии защиты информации в вычислительных сетях	4				Лекция		Работа с лекционным материалом и учебной литературой	Класс с медиаоборудованием	Собеседование (устный опрос)	1-3
	Разработка программы, реализующую симметричную криптосистему		4		4	Компьютерный практикум	26	Подготовка к практическим занятиям и отчета по работе	Лаборатория с компьютерами	Отчет по практической работе	1-3
	Модели безопасности информационных систем	4				Лекция	18	Работа с лекционным материалом и учебной литературой	Класс с медиаоборудованием	Собеседование (устный опрос)	1-3
Политика информационной безопасности	Анализ безопасности информации в корпоративной информационной системе	4				Лекция	18	Работа с лекционным материалом и учебной литературой	Класс с медиаоборудованием	Собеседование (устный опрос)	1-3
	Основы разработки политики информационной безопасности	4				Лекция		Работа с лекционным материалом и учебной литературой	Класс с медиаоборудованием	Собеседование (устный опрос)	1-3
	Разработка политики информационной безопасности организации			8	8	Компьютерный практикум	24	Подготовка к практическим занятиям и отчета по работе	Лаборатория с компьютерами	Отчет по практической работе (защита) Зачет по вопросам в письменной форме	1-3
Итого:		34	8	50			160				
		252									

5. Критерии и нормы текущего контроля и промежуточной аттестации

Формы текущего контроля	Условия допуска	Критерии и нормы оценки
лекция: «Симметричная криптографическая система»	Допускаются все	«зачтено» - студент продемонстрировал знания по изучаемой теме дисциплины; «не зачтено» - студент не продемонстрировал знания по изучаемой теме дисциплины
практ. занятие: «Разработка программы по реализации блочного симметричного алгоритма шифрования»	Допускаются все	«зачтено» - студент продемонстрировал работу программы, соответствующей заданию; предоставлен отчет о выполнении работы, оформленный в соответствии с установленными требованиями; продемонстрировал знания по изучаемой теме дисциплины и умение уверенно применять их на практике; обосновывает принятые решения; понимает и может объяснить код программы; «не зачтено» - студент не продемонстрировал работу программы, соответствующей заданию; не предоставил отчет о выполнении работы, оформленный в соответствии с установленными требованиями; не продемонстрировал знания по изучаемой теме дисциплины и умение применять их на практике; не может обосновывать принятые решения; не может объяснить код программы;
практ. занятие: «Разработка программы шифрования и дешифрирования произвольного файла по алгоритму создания цепочек OFB»	Допускаются все	«зачтено» - студент продемонстрировал работу программы, соответствующей заданию; предоставлен отчет о выполнении работы, оформленный в соответствии с установленными требованиями; продемонстрировал знания по изучаемой теме дисциплины и умение уверенно применять их на практике; обосновывает принятые решения; понимает и может объяснить код программы; «не зачтено» - студент не продемонстрировал работу программы, соответствующей заданию; не предоставил отчет о выполнении работы, оформленный в соответствии с установленными требованиями; не продемонстрировал знания по изучаемой теме дисциплины и умение применять их на практике; не может обосновывать принятые решения; не может объяснить код программы;

практ. занятие: «Разработка программы реализации алгоритма хеширования для создания ключа на основе пароля»	Допускаются все	«зачтено» - студент продемонстрировал работу программы, соответствующей заданию; предоставлен отчет о выполнении работы, оформленный в соответствии с установленными требованиями; продемонстрировал знания по изучаемой теме дисциплины и умение уверенно применять их на практике; обосновывает принятые решения; понимает и может объяснить код программы; «не зачтено» - студент не продемонстрировал работу программы, соответствующей заданию; не предоставил отчет о выполнении работы, оформленный в соответствии с установленными требованиями; не продемонстрировал знания по изучаемой теме дисциплины и умение применять их на практике; не может обосновывать принятые решения; не может объяснить код программы;
практ. занятие: «Разработка подсистемы шифрования для симметричной криптосистемы»	Допускаются все	«зачтено» - студент продемонстрировал работу программы, соответствующей заданию; предоставлен отчет о выполнении работы, оформленный в соответствии с установленными требованиями; продемонстрировал знания по изучаемой теме дисциплины и умение уверенно применять их на практике; обосновывает принятые решения; понимает и может объяснить код программы; «не зачтено» - студент не продемонстрировал работу программы, соответствующей заданию; не предоставил отчет о выполнении работы, оформленный в соответствии с установленными требованиями; не продемонстрировал знания по изучаемой теме дисциплины и умение применять их на практике; не может обосновывать принятые решения; не может объяснить код программы;
практ. занятие: «Разработка подсистемы дешифрирования для симметричной криптосистемы»	Допускаются все	«зачтено» - студент продемонстрировал работу программы, соответствующей заданию; предоставлен отчет о выполнении работы, оформленный в соответствии с установленными требованиями; продемонстрировал знания по изучаемой теме дисциплины и умение уверенно применять их на практике; обосновывает принятые решения; понимает и может объяснить код программы; «не зачтено» - студент не продемонстрировал работу программы, соответствующей заданию; не предоставил отчет о выполнении работы, оформленный в соответствии с установленными требованиями; не про-

		демонстрировал знания по изучаемой теме дисциплины и умение применять их на практике; не может обосновывать принятые решения; не может объяснить код программы;
лекция: «Асимметричная криптографическая система»	Допускаются все	«зачтено» - студент продемонстрировал знания по изучаемой теме дисциплины; «не зачтено» - студент не продемонстрировал знания по изучаемой теме дисциплины
лабор. работа: «Разработка программы сжатия данных с целью уменьшения энтропии информации по алгоритму RLE или LZW»	Допускаются все	«зачтено» - студент продемонстрировал работу программы, соответствующей заданию; предоставлен отчет о выполнении работы, оформленный в соответствии с установленными требованиями; продемонстрировал знания по изучаемой теме дисциплины и умение уверенно применять их на практике; обосновывает принятые решения; понимает и может объяснить код программы; «не зачтено» - студент не продемонстрировал работу программы, соответствующей заданию; не предоставил отчет о выполнении работы, оформленный в соответствии с установленными требованиями; не продемонстрировал знания по изучаемой теме дисциплины и умение применять их на практике; не может обосновывать принятые решения; не может объяснить код программы;
лекция: «Стандарты информационной безопасности»	Допускаются все	«зачтено» - студент продемонстрировал знания по изучаемой теме дисциплины; «не зачтено» - студент не продемонстрировал знания по изучаемой теме дисциплины
лекция: «Базовые технологии защиты информации в вычислительных сетях»	Допускаются все	«зачтено» - студент продемонстрировал знания по изучаемой теме дисциплины; «не зачтено» - студент не продемонстрировал знания по изучаемой теме дисциплины
лабор. работа: «Разработка программы, реализующую симметричную криптосистему»	Допускаются все	«зачтено» - студент продемонстрировал работу программы, соответствующей заданию; предоставлен отчет о выполнении работы, оформленный в соответствии с установленными требованиями; продемонстрировал знания по изучаемой теме дисциплины и умение уверенно применять их на практике; обосновывает принятые решения; понимает и может

		объяснить код программы; «не зачтено» - студент не продемонстрировал работу программы, соответствующей заданию; не предоставил отчет о выполнении работы, оформленный в соответствии с установленными требованиями; не продемонстрировал знания по изучаемой теме дисциплины и умение применять их на практике; не может обосновывать принятые решения; не может объяснить код программы;
лекция: «Модели безопасности информационных систем»	Допускаются все	«зачтено» - студент продемонстрировал знания по изучаемой теме дисциплины; «не зачтено» - студент не продемонстрировал знания по изучаемой теме дисциплины
лекция: «Анализ безопасности информации в корпоративной информационной системе»	Допускаются все	«зачтено» - студент продемонстрировал знания по изучаемой теме дисциплины; «не зачтено» - студент не продемонстрировал знания по изучаемой теме дисциплины
лекция: «Основы разработки политики информационной безопасности»	Допускаются все	«зачтено» - студент продемонстрировал знания по изучаемой теме дисциплины; «не зачтено» - студент не продемонстрировал знания по изучаемой теме дисциплины
практ. занятие: «Разработка политики информационной безопасности организации»	Допускаются все	«зачтено» - студент продемонстрировал работу программы, соответствующей заданию; предоставлен отчет о выполнении работы, оформленный в соответствии с установленными требованиями; продемонстрировал знания по изучаемой теме дисциплины и умение уверенно применять их на практике; обосновывает принятые решения; понимает и может объяснить код программы; «не зачтено» - студент не продемонстрировал работу программы, соответствующей заданию; не предоставил отчет о выполнении работы, оформленный в соответствии с установленными требованиями; не продемонстрировал знания по изучаемой теме дисциплины и умение применять их на практике; не может обосновывать принятые решения; не может объяснить код программы;

Форма проведения промежуточной аттестации	Условия допуска	Критерии и нормы оценки
Зачет по вопросам в письменной форме	Выполнено не менее 50% работ по дисциплине, сданы все необходимые отчеты по ним	«зачтено» - студент знает базовые термины, понятия и теоретические основы по темам дисциплины, владеет основными вопросами по темам дисциплины, выполнял лабораторные и практические работы на достаточном уровне, в основном разбирается в темах дисциплины, вынесенных на самостоятельное изучение «незачтено» - студент не посещал аудиторные занятия без уважительной причины, не знает наиболее важные определения и не владеет знаниями по основным вопросам изучаемой дисциплины, выполнял практические и лабораторные работы на низком уровне, слабо разбирается в вопросах, вынесенных на самостоятельное изучение

6. Критерии и нормы оценки курсовых работ (проектов)

По учебному курсу данный подраздел не предусмотрен.

7. Примерная тематика письменных работ (курсовых, рефератов, контрольных, расчетно-графических и др.)

По учебному курсу данный подраздел не предусмотрен.

8. Вопросы к зачету

1. Методы защиты информации от несанкционированного изменения структуры систем
2. Источники, риски и формы атак на информацию
3. Организационные методы защиты информации.
4. Блочный шифр ГОСТ 28147-89
5. Алгоритмы архивации Хаффмана.
6. Алгоритмы архивации Лемпеля-Зива
7. Алгоритмы архивации RLE
8. Транспортное кодирование.
9. Хеширование паролей.
10. Общая схема симметричной криптосистемы
11. Общая схема асимметричной криптосистемы.
12. Алгоритм вычисления хеш-функции согласно ГОСТ Р 34.11-2012
13. ЭЦП с дополнительными свойствами.
14. Классификация процессов аутентификации.
15. Основы биометрической аутентификации и идентификации
16. Основы администрирования вычислительных сетей
17. Расчет рисков информационной безопасности
18. Методы внесения случайности в сообщения
19. Асимметричный алгоритм шифрования RSA
20. Основная законодательная база в области информационных технологий
21. Международные стандарты информационной безопасности
22. Основы хеширование и хранения паролей
23. Дискреционная модель Харрисона-Рузо-Ульмана
24. Реализация системы разграничения доступа в операционных системах
25. Основные пути получения информации о системе защиты информации
26. Понятие политики информационной безопасности
27. Режимы шифрования
28. Требования защищенности средств вычислительной техники от несанкционированного доступа к информации
29. Алгоритм Меркеля-Дамгарда по реализации хеш-функции
30. Алгоритм формирования ЭЦП по ГОСТ Р 34.10-2012
31. Основные понятия и определения безопасности информации.
32. Классификация угроз безопасности информации

33. Классификация методов противодействия угрозам безопасности информации.
34. Правовые методы защиты информации
35. Методы защиты информации от случайных угроз.
36. Методы защиты информации от шпионажа и диверсий.
37. Методы защиты информации от электромагнитных излучений и наводок.
38. Методы защиты информации от несанкционированного доступа.
39. Концепции построения систем разграничения доступа.
40. Криптографические методы защиты
41. Основы симметричных криптоалгоритмов.
42. Криптоалгоритм на основе сети Файстеля.
43. Блочный шифр DES
44. Алгоритмы создания цепочек.
45. Методы рандомизации сообщений.
46. Классификация алгоритмов архивации данных
47. Хеш-функция и её реализация
48. Понятие симметричной криптосистемы и ее функции
49. Асимметричные криптоалгоритмы
50. Асимметричный алгоритм шифрования RSA.
51. Электронная цифровая подпись
52. Основные понятия идентификации и аутентификации
53. Простая аутентификация
54. Методы строгой аутентификации.
55. Стандарты информационной безопасности.
56. Базовые технологии защиты информации в вычислительных сетях.
57. Модели безопасности операционных систем
58. Классификация информационных объектов по категориям информационной безопасности
59. Требования к системам защиты информации.
60. Порядок разработки политики информационной безопасности.
61. Многоуровневая защита систем обработки информации.

9. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

9.1 Паспорт фонда оценочных средств

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1	Модуль 1. Криптографические алгоритмы защиты информации в корпоративных информационных системах	ПК-4, ПК-5	Отчет по практической работе Отчет по практической работе (защита) Собеседование (устный опрос)
2	Модуль 2. Стандарты информа-	ПК-4, ПК-5	Отчет по практической

	ционной безопасности и модели безопасности информационных систем		работе Собеседование (устный опрос)
3	Модуль 3. Политика информационной безопасности	ПК-4, ПК-5	Зачет по вопросам в письменной форме Отчет по практической работе (защита) Собеседование (устный опрос)

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

Вопросы для собеседования по модулю (примеры вопросов)

Модуль 1. Криптографические алгоритмы защиты информации в корпоративных информационных системах

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.
12. Что такое криптография, криптоанализ и криптология?
13. Что такое криптосистема?
14. Перечислите и охарактеризуйте методы криптографических преобразований.
15. Дайте классификацию криптоалгоритмов.
16. Дайте понятие основных операций, используемых в алгоритмах шифрования.
17. Дайте понятие потокового и блочного шифра.
18. Перечислите операции, используемые в алгоритмах блочных шифров.
19. Приведите схему шифрования и дешифрирования по сети Фейстеля.
20. ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.
21. Что такое режимы шифрования?
22. Раскройте принцип реализации режима шифрования обратная связь по выходу (OFB).

23. Раскройте принципы внесения случайности в сообщения при шифровании.
24. Приведите способы генерации случайных чисел.
25. Понятие и свойства Хеш-функции.
26. Приведите пример алгоритма приведения пароля пользователя к заданной длине ключа с помощью Хеш-функции.
27. Приведите общую схема симметричной криптосистемы.
28. Основная идея асимметричных криптоалгоритмов?
29. Приведите необходимые условия реализации асимметричной криптографии.
30. Приведите примеры асимметричных критоалгоритмов.
31. Общая схема асимметричной криптосистемы.
32. Первый этап алгоритма RSA по созданию пары ключей.
33. Этап передачи зашифрованного сообщения в алгоритме RSA.
34. Понятие и свойства Хеш-функции.
35. Приведите примеры использования и реализаций криптографических Хеш-функций.
36. Раскройте алгоритм Меркеля-Дамгарда по реализации хеш-функции.
37. Алгоритм вычисления хеш-функции согласно ГОСТ Р 34.11-2012.
38. Схема алгоритма Девиса и Майера для хеширования паролей.
39. Назначение и виды защиты от злоумышленных действий при использовании ЭЦП.
40. Алгоритм формирования и проверки ЭЦП.
41. Алгоритм формирования ЭЦП по ГОСТ Р 34.10-2012.

Модуль 2. Стандарты информационной безопасности и модели безопасности информационных систем

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 и дайте понятия базовых технологий защиты информации.
11. Дайте классификацию процессов аутентификации.

12. В чем заключается строгая аутентификация.
13. В чем заключается простая аутентификация.
14. Основы биометрической аутентификации.
15. Что такое Хеширование пароля?
16. Дайте характеристики криптографических хеш-функций.
17. Дайте характеристики методов простой и биометрической аутентификации.
18. Приведите алгоритм строгой аутентификации на основе симметричных алгоритмов.
19. Что такое Модель политики информационной безопасности?
20. Приведите классы модели политики информационной безопасности.
21. Раскройте дискреционную модель Харрисона-Рузо-Ульмана.
22. Что такое матричное разграничения доступа. Приведите пример реализации.
23. Что такое мандатное разграничение доступа. Приведите пример реализации.

Модуль 3. Политика информационной безопасности

1. Перечислите основные пути получения информации о системе защиты?
2. Дайте классификацию информационных объектов по требуемой степени безотказности.
3. Дайте классификацию информационных объектов по уровню конфиденциальности.
4. Что такое риск информационной безопасности и как он вычисляется.
5. Перечислите уровни ущерба от реализации рисков.
6. Приведите пример формирования оценки вероятности атак на информацию.
7. Дайте алгоритм расчета риска информационной безопасности
8. Что такое политика информационной безопасности?
9. Перечислите требования к системе безопасности.
10. Раскройте принципа доступа к информационным ресурсам организации.
11. Опишите основные направления разработки политики безопасности.
12. Перечислите этапы разработки политики информационной безопасности

Критерии оценки:

- оценка «зачтено» выставляется студенту, если продемонстрированы всесторонние, систематизированные, глубокие знания по поставленным вопросам;

- оценка «не зачтено»выставляется студенту, если продемонстрированы фрагментарные, несистематизированные знания по поставленным вопросам.

1.1.1 Комплект отчетов по практическим работам (примеры)

Практическое занятие №1 «Разработка программы по реализации блочного симметричного алгоритма шифрования»

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 дешифрирования произвольного 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 хеширования 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 симметричной криптосистемы»

Форма отчета по практическому занятию №4

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

Практическое занятие №5 «Разработка подсистемы дешифрирования для симметричной криптосистемы»

Форма отчета по практическому занятию №5

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

Практическое занятие №6 «Разработка политики информационной безопасности организации»

Форма отчета по практическому занятию №6

- 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:

оценка «зачтено» ставится студенту, который продемонстрировал результаты выполнения работы, соответствующие поставленному заданию, и предоставил отчет, оформленный должным образом и содержащий краткое описание полученных результатов;

оценка «не зачтено» ставится студенту, который не продемонстрировал результаты выполнения работы или не представил по ней отчет или представленный отчет не соответствует требованиям по оформлению.

10. Образовательные технологии и методические указания по освоению дисциплины (учебного курса)

В рамках изучения дисциплины предусмотрено использование следующих образовательных технологий:

- технология традиционного обучения;

- интерактивные технологии: учебные дискуссии (применяются во всех модулях по итогам выполнения заданий).

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 кода.

11. Учебно-методическое и информационное обеспечение дисциплины (учебного курса)

11.1 Обязательная литература

№ п/п	Библиографическое описание	Тип (учебник, учебное пособие, учебно-методическое пособие, практикум, др.)	Количество в библиотеке

11.2 Дополнительная литература и учебные материалы (аудио-, видеопособия и др.)

- фонд научной библиотеки ТГУ:

№ п/п	Библиографическое описание	Тип (учебник, учебное пособие, учебно-методическое пособие, практикум, аудио-, видеопособия и др.)	Количество в библиотеке
1	Баранова Е. К. Информационная безопасность и защита информации [Электронный ресурс] : учеб. пособие / Е. К. Баранова, А. В. Бабаш. - 3-е изд., перераб. и доп. - Москва : РИОР : ИНФРА-М, 2017. - 322 с. : ил. - (Высшее образование). - ISBN 978-5-369-01450-	Учебное пособие	ЭБС «Znanium.com»
2	Горюхина Е. Ю. Информационная безопасность [Электронный ресурс] : учеб. пособие / Е. Ю. Горюхина, Л. И. Литвинова, Н. В. Ткачева ; Воронеж. гос. аграр. ун-т им. Императора Петра I. - Воронеж : ВГАУ им. Петра I, 2015. - 220 с.	Учебное пособие	ЭБС «IPRbooks»
3	Джонс К. Д. Инструментальные	Учебное пособие	ЭБС

	средства обеспечения безопасности [Электронный ресурс] : [курс лекций] / К. Д. Джонс, М. Шема, Б. С. Джонсон. - 2-е изд., испр. - Москва : ИНТУИТ, 2016. - 915 с. : ил.		«IPRbooks»
4	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	ЭБС «IPRbooks»
5	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	ЭБС «IPRbooks»
6	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	ЭБС «IPRbooks»
7	Технологии защиты информации в компьютерных сетях [Электронный ресурс] / Н. А. Руденков [и др.]. - 2-е изд., испр. - Москва : ИНТУИТ, 2016. - 369 с. : ил.	Учебное пособие	ЭБС «IPRbooks»
8	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	ЭБС «IPRbooks»

- другие фонды:

№ п/п	Библиографическое описание	Тип (учебник, учебное пособие, учебно-методическое пособие, практикум, аудио-, видеопособия и др.)	Место хранения (методический кабинет кафедры, городские библиотеки и др.)

СОГЛАСОВАНО

Директор научной библиотеки _____ _____

(подпись) *(И.О. Фамилия)*

«___»_____20___г.

МП

11.3 Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

1. Hacking Everything. Режим доступа: http://www.gomzin.com/cryptogram.html, 2016-01-01.
2. The Tiny Encryption Algorithm (TEA). Режим доступа: http://143.53.36.235:8080/tea.htm, 2016-01-01.
3. Библиотека: Защита информации, криптография. Режим доступа: http://www.win-ni.narod.ru/biblio/cryptobib.htm, 2016-01-01.
4. ДОКТРИНА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ. Режим доступа: http://www.scrf.gov.ru/documents/5.html, 2016-01-01.
5. Режимы шифрования Олег Зензин. Режим доступа: http://citforum.ru/security/cryptography/rejim_shifrov/, 2016-01-01.
6. Сайт Брюса Шнайера. Schneier on Security. Режим доступа: https://www.schneier.com/, 2016-01-01.
7. Федеральная служба по техническому и экспортному контролю. Режим доступа: http://fstec.ru/, 2016-01-01.

11.4 Перечень программного обеспечения

№ п/п	Наименование ПО	Количество лицензий	Реквизиты договора (дата, номер, срок действия)
1	Microsoft DreamSpark версия Premium	1	652/2014 от 07.07.2014
2	Microsoft Office Standart 2007 версия 2007	неограниченный	
3	Microsoft Windows 7 версия 7	30	Бесплатно для учебных организаций

11.5 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий	Перечень основного оборудования	Фактический адрес учебных кабинетов, лабораторий, мастерских и др.	Площадь, $м^2$	Количество посадочных мест
1	Компьютерный класс. Помещение для самостоятельной работы. Учебная аудитория	Столы ученические, стулья ученические, ПК с выходом в сеть Интернет	445667 Самарская область, г.Тольятти, Центральный р-н, ул.	84,8	16

	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.		Белорус-ская, д.14, позиция по ТП №48, 4 этаж, Г-401		
2	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 Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации.	Компьютер (монитор 19”, системный блок Pentium (R) Dual-Core E5500 2,8 GHz / 4 Gb / 500 Gb) , стол ученический, стол компьютерный, стол преподавательский, стулья, Доска аудиторная(меловая).	445667 Самарская область, г.Тольятти, Центральный р-н, ул. Белорусская, д.16В, позиция по ТП №31, 4 этаж, УЛК-401	49,5	24
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.	Стол ученический двухместный (моноблок), доска аудиторная 3-х секционная (меловая), стол преподавательский, стул, проектор Acer	445667 Самарская область, г.Тольятти, Центральный р-н, ул. Белорусская, д.16В, позиция по ТП №50, 4 этаж, УЛК-418	90,6	80

	Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации.				