

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГБОУ ВО «КАБАРДИНО-БАЛКАРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
им. Х. М. БЕРБЕКОВА» (КБГУ)**

Институт информатики, электроники и робототехники

Кафедра информационных технологий в управлении техническими системами

СОГЛАСОВАНО

УТВЕРЖДАЮ

Руководитель ОПОП _____ В. А. Хакулов

Директор института _____ Н. В. Черкесова

« _____ » _____ 2020 г.

« _____ » _____ 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.07 «Защита информации в технических системах»

Направление подготовки

27.03.04 Управление в технических системах
(код и наименование направления подготовки)

Профиль подготовки

Информационные технологии в управлении техническими системами
(наименование профиля подготовки)

Квалификация (степень) выпускника:

бакалавр

Форма обучения

очная

Нальчик 2020

Рабочая программа дисциплины «Защита информации в технических системах»
/ сост. В. А. Шаповалов – Нальчик: КБГУ, 2020. – 60 с.

(год составления и количество страниц рабочей программы)

Рабочая программа предназначена для преподавания вариативной части блока Б1 студентам очной формы обучения по направлению подготовки 27.03.04 «Управление в технических системах», 7 семестр, 4 курса.

Рабочая программа составлена с учетом федерального государственного образовательного стандарта высшего образования по направлению подготовки 27.03.04 «Управление в технических системах» утвержденного приказом Министерства образования и науки Российской Федерации № 1171 от 20.10.2015 г.

(дата и номер приказа)

© Шаповалов В. А. 2019
© ФГБОУ КБГУ, 2019

Содержание

1. Цели и задачи освоения дисциплины	4
2. Место дисциплины в структуре ООП ВПО	4
3. Требования к результатам освоения содержания дисциплины	4
4. Содержание и структура дисциплины (модуля).....	5
4.1. Содержание разделов дисциплины.....	5
4.2. Структура дисциплины	8
4.3. Лабораторные работы	10
4.4 Самостоятельная работа	14
5. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации.	15
5.1 Оценочные материалы для текущего контроля успеваемости	15
5.2. Оценочные материалы для промежуточной аттестации	48
6. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности.....	50
6.1 Результаты освоения учебной дисциплины, подлежащие проверке.....	50
6.2 Шкала оценивания планируемых результатов обучения.	52
7. Учебно-методическое обеспечение дисциплины	53
7.1. Основная литература.....	53
7.2. Дополнительная литература.	54
7.3 Интернет-ресурсы.....	55
7.4. Перечень учебно-методических разработок.....	56
7.5 Перечень профессиональных баз данных и информационно-справочных систем.....	56
7.6 Программное обеспечение современных информационно-коммуникационных технологий.....	56
8. Материально-техническое обеспечение дисциплины.	57
9. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья.	58

1. Цели и задачи освоения дисциплины

Цель преподавания дисциплины «Защита информации в технических системах» заключается в том, чтобы ознакомить студентов с основными понятиями и определениями информационной безопасности; источниками, рисками и формами атак на информацию; угрозами, которыми подвергается информация; вредоносными программами; защитой от компьютерных вирусов и других вредоносных программ; методами и средствами защиты информации; политикой безопасности компаний в области информационной безопасности; стандартами информационной безопасности; криптографическими методами и алгоритмами шифрования информации; алгоритмами аутентификации пользователей; защитой информации от утечки; требованиям к системам защиты информации.

Задачами дисциплины является ознакомить студентов с тенденциями развития защиты информационной с моделями возможных угроз, терминологией и основными понятиями теории защиты информации, а так же с нормативными документами и методами защиты компьютерной информации.

2. Место дисциплины в структуре ООП ВПО

Дисциплина «Защита информации в технических системах» относится к вариативной части профессионального цикла дисциплин Б.1 рабочего учебного плана по направлению 27.03.04 «Управление в технических системах», и изучается в 7 семестре 4 курса.

3. Требования к результатам освоения содержания дисциплины

В процессе изучения дисциплины «Защита информации в технических системах» у студентов по направлению подготовки 27.03.04 «Управление в технических системах» с квалификацией (степенью) «бакалавр» должны быть сформированы профессиональные компетенции.

Профессиональные компетенции (ПК):

- готовность к участию в работах по изготовлению, отладке и сдаче в эксплуатацию систем и средств автоматизации и управления **(ПК-10)**;
- готовность участвовать в разработке и изготовлении стендов для комплексной отладки и испытаний программно-аппаратных управляющих комплексов **(ПК-13)**;
- способностью участвовать в монтаже, наладке, настройке, проверке и сдаче опытных образцов программно-аппаратных средств и комплексов автоматизации и управления **(ПК-14)**.

В результате изучения дисциплины «Защита информации в технических системах»

студент:

Должен знать теоретические составляющие защиты информации.

Должен уметь выявлять источники, риски и формы атак на информацию, работать в соответствии со стандартами безопасности, использовать криптографические модели, алгоритмы шифрования информации и аутентификации пользователей, составлять многоуровневую защиту данных.

Должен владеть навыками проектирования систем защиты информации.

4. Содержание и структура дисциплины (модуля)

4.1. Содержание разделов дисциплины

№ Раздела	Наименование раздела	Содержание раздела	Формируемая компетенция (часть компетенции)	Оценочные средства
1	2	3	4	5
1.	Средства и методы защиты информации.	Классификация средств защиты информации и программного обеспечения от несанкционированного доступа и копирования. Активные и пассивные методы защиты программного обеспечения. Идентификация электронной подписи. Аутентификация. Особенности изготовления, отладки и сдачи в эксплуатацию систем и средств автоматизации и управления защитой информации в технических системах. (готовность к участию в работах по изготовлению, отладке и сдаче в эксплуатацию систем и средств автоматизации и управления, готовность участвовать в разработке и изготовлении стендов для комплексной отладки и испытаний программно-аппаратных управляющих комплексов, способностью участвовать в монтаже, наладке, настройке, проверке и сдаче опытных образцов программно-	ПК-10 ПК-13 ПК-14	лабораторная работа, вопросы на коллоквиуме, тесты, защита реферата, экзамен.

		аппаратных средств и комплексов автоматизации и управления).		
2.	Криптография и шифрование в области защиты информации.	Основы криптографии. Методы и стандарты шифрования данных в вычислительных системах. Разработка и изготовление стендов для комплексной отладки и испытаний программно-аппаратных управляющих комплексов криптографической обработки данных. (готовность к участию в работах по изготовлению, отладке и сдаче в эксплуатацию систем и средств автоматизации и управления, готовность участвовать в разработке и изготовлении стендов для комплексной отладки и испытаний программно-аппаратных управляющих комплексов, способностью участвовать в монтаже, наладке, настройке, проверке и сдаче опытных образцов программно-аппаратных средств и комплексов автоматизации и управления).	ПК-10 ПК-13 ПК-14	лабораторная работа, вопросы на коллоквиуме, тесты, защита реферата, экзамен.
3.	Сжатие данных как способ кодирования.	Обзор методов сжатия данных. Сжатие данных со словарем. (готовность к участию в работах по изготовлению, отладке и сдаче в эксплуатацию систем и средств автоматизации и управления, готовность участвовать в разработке и изготовлении стендов для комплексной отладки и испытаний программно-аппаратных управляющих комплексов, способностью участвовать в монтаже, наладке, настройке, проверке и сдаче опытных образцов программно-аппаратных средств и комплексов автоматизации и управления).	ПК-10 ПК-13 ПК-14	лабораторная работа, вопросы на коллоквиуме, тесты, защита реферата, экзамен.

4.	Компьютерные вирусы.	<p>Классификация компьютерных вирусов. Организационные и программные способы борьбы с вирусным заражением программного обеспечения. Антивирусные программные средства. Монтаж, наладка, настройка, проверка и сдача опытных образцов программно-аппаратных средств и комплексов автоматизации и управления защитой информации. (готовность к участию в работах по изготовлению, отладке и сдаче в эксплуатацию систем и средств автоматизации и управления, готовность участвовать в разработке и изготовлении стендов для комплексной отладки и испытаний программно-аппаратных управляющих комплексов, способностью участвовать в монтаже, наладке, настройке, проверке и сдаче опытных образцов программно-аппаратных средств и комплексов автоматизации и управления).</p>	<p>ПК-10 ПК-13 ПК-14</p>	<p>лабораторная работа, вопросы на коллоквиуме, тесты, защита реферата, экзамен.</p>
5.	Правовые основы защиты информации.	<p>Применение патентования и норм авторского права при защите программных продуктов. Основные положения Закона об охране программ для ЭВМ и баз данных. (готовность к участию в работах по изготовлению, отладке и сдаче в эксплуатацию систем и средств автоматизации и управления, готовность участвовать в разработке и изготовлении стендов для комплексной отладки и испытаний программно-аппаратных управляющих комплексов, способностью участвовать в монтаже, наладке, настройке, проверке и сдаче опытных образцов программно-аппаратных средств и комплексов автоматизации и управления).</p>	<p>ПК-10 ПК-13 ПК-14</p>	<p>лабораторная работа, вопросы на коллоквиуме, тесты, защита реферата, экзамен.</p>

		образцов программно-аппаратных средств и комплексов автоматизации и управления).		
--	--	--	--	--

4.2. Структура дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 часа).
Промежуточная аттестация – экзамен (7 семестр).

Вид работы	Трудоемкость, часов	
	семестр № 7	Всего
Общая трудоемкость	144	144
Аудиторная работа:	56	56
<i>Лекции (Л)</i>	14	14
<i>Практические занятия (ПЗ)</i>	-	-
<i>Лабораторные работы (ЛР)</i>	42	42
Самостоятельная работа:	61	61
Курсовой проект (КП), курсовая работа (КР)	-	-
Расчетно-графическое задание (РГЗ)	-	-
Реферат (Р)	4	4
Эссе (Э)	-	-
Самостоятельное изучение разделов	47	47
Контрольная работа (К)	-	-
Самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям, коллоквиумам, рубежному контролю и т.д.)	10	10
Подготовка и сдача экзамена	27	27
Вид итогового контроля (зачет, экзамен)	Экзамен	Экзамен

Разделы дисциплины

№ раздела	Наименование раздела	Количество часов			
		Всего	Ауд. работа		Вне ауд. раб. (СР)
			Л	ЛР	
1	2	3	4	5	6
1.	Средства и методы защиты информации. (готовность к участию в работах по изготовлению, отладке и сдаче в эксплуатацию систем и средств автоматизации и управления, готовность участвовать в разработке и изготовлении стендов для комплексной отладки и испытаний программно-аппаратных управляющих комплексов, способностью участвовать в монтаже, наладке, настройке, проверке и сдаче опытных образцов программно-аппаратных средств и комплексов автоматизации и управления).	27	2	10	15
2.	Криптография и шифрование в области защиты информации. (готовность к участию в работах по изготовлению, отладке и сдаче в эксплуатацию систем и средств автоматизации и управления, готовность	38	4	14	20

	участвовать в разработке и изготовлении стендов для комплексной отладки и испытаний программно-аппаратных управляющих комплексов, способностью участвовать в монтаже, наладке, настройке, проверке и сдаче опытных образцов программно-аппаратных средств и комплексов автоматизации и управления).				
3.	Сжатие данных как способ кодирования. (готовность к участию в работах по изготовлению, отладке и сдаче в эксплуатацию систем и средств автоматизации и управления, готовность участвовать в разработке и изготовлении стендов для комплексной отладки и испытаний программно-аппаратных управляющих комплексов, способностью участвовать в монтаже, наладке, настройке, проверке и сдаче опытных образцов программно-аппаратных средств и комплексов автоматизации и управления).	15	4	3	8
4.	Компьютерные вирусы. (готовность к участию в работах по изготовлению, отладке и сдаче в эксплуатацию систем и средств автоматизации и управления, готовность участвовать в разработке и изготовлении стендов для комплексной отладки и испытаний программно-аппаратных управляющих комплексов, способностью участвовать в монтаже, наладке, настройке, проверке и сдаче опытных образцов программно-аппаратных средств и комплексов автоматизации и управления).	31	3	13	15
5.	Правовые основы защиты информации. (готовность к участию в работах по изготовлению, отладке и сдаче в эксплуатацию систем и средств автоматизации и управления, готовность участвовать в разработке и изготовлении стендов для комплексной отладки и испытаний программно-аппаратных управляющих комплексов, способностью участвовать в монтаже, наладке, настройке, проверке и сдаче опытных образцов программно-аппаратных средств и комплексов автоматизации и управления).	6	1	2	3
Итого:		117	14	42	61
6.	Контроль (подготовка и сдача экзамена)	27	-	-	-
Всего:		144			

4.3. Лабораторные работы

№ занятия	№ раздела	Тема	Кол-во часов
1	2	3	4
1.	1	Исследование возможностей системы безопасности Windows XP по разграничению полномочий пользователей. (готовность к участию в работах по изготовлению, отладке и сдаче в эксплуатацию систем и средств автоматизации и управления, готовность участвовать в разработке и изготовлении стендов для комплексной отладки и испытаний программно-аппаратных управляющих комплексов, способностью участвовать в монтаже, наладке, настройке, проверке и сдаче	1

		опытных образцов программно-аппаратных средств и комплексов автоматизации и управления).	
2.	1	Исследование авторизации пользователей в Windows XP. (готовность к участию в работах по изготовлению, отладке и сдаче в эксплуатацию систем и средств автоматизации и управления, готовность участвовать в разработке и изготовлении стендов для комплексной отладки и испытаний программно-аппаратных управляющих комплексов, способностью участвовать в монтаже, наладке, настройке, проверке и сдаче опытных образцов программно-аппаратных средств и комплексов автоматизации и управления).	1
3.	1	Реализация дискреционной модели политики безопасности. (готовность к участию в работах по изготовлению, отладке и сдаче в эксплуатацию систем и средств автоматизации и управления, готовность участвовать в разработке и изготовлении стендов для комплексной отладки и испытаний программно-аппаратных управляющих комплексов, способностью участвовать в монтаже, наладке, настройке, проверке и сдаче опытных образцов программно-аппаратных средств и комплексов автоматизации и управления).	1
4.	1	Процедура аутентификации пользователя на основе пароля. (готовность к участию в работах по изготовлению, отладке и сдаче в эксплуатацию систем и средств автоматизации и управления, готовность участвовать в разработке и изготовлении стендов для комплексной отладки и испытаний программно-аппаратных управляющих комплексов, способностью участвовать в монтаже, наладке, настройке, проверке и сдаче опытных образцов программно-аппаратных средств и комплексов автоматизации и управления).	1
5.	1	Изучение методов парольной защиты данных. (готовность к участию в работах по изготовлению, отладке и сдаче в эксплуатацию систем и средств автоматизации и управления, готовность участвовать в разработке и изготовлении стендов для комплексной отладки и испытаний программно-аппаратных управляющих комплексов, способностью участвовать в монтаже, наладке, настройке, проверке и сдаче опытных образцов программно-аппаратных средств и комплексов автоматизации и управления).	2
6.	1	Оценка степени стойкости парольной защиты. (готовность к участию в работах по изготовлению, отладке и сдаче в эксплуатацию систем и средств автоматизации и управления, готовность участвовать в разработке и изготовлении стендов для комплексной отладки и испытаний программно-аппаратных управляющих комплексов, способностью участвовать в монтаже, наладке, настройке, проверке и сдаче опытных образцов программно-аппаратных средств и комплексов автоматизации и управления).	2
7.	1	Методы и средства защиты компьютерной информации в процессе изготовления, отладки и сдачи в эксплуатацию систем и средств автоматизации и управления. (готовность к участию в работах по изготовлению, отладке и сдаче в эксплуатацию систем и средств автоматизации и управления, готовность участвовать в разработке и изготовлении стендов для комплексной отладки и испытаний программно-аппаратных управляющих комплексов, способностью участвовать в монтаже, наладке, настройке, проверке и сдаче опытных образцов программно-аппаратных средств и комплексов автоматизации и управления).	2

		комплексов автоматизации и управления).	
8.	2	Основы криптографической защиты информации Шифр замены. (готовность к участию в работах по изготовлению, отладке и сдаче в эксплуатацию систем и средств автоматизации и управления, готовность участвовать в разработке и изготовлении стендов для комплексной отладки и испытаний программно-аппаратных управляющих комплексов, способностью участвовать в монтаже, наладке, настройке, проверке и сдаче опытных образцов программно-аппаратных средств и комплексов автоматизации и управления).	2
9.	2	Взлом моноалфавитного подстановочного шифра методом частотной атаки. (готовность к участию в работах по изготовлению, отладке и сдаче в эксплуатацию систем и средств автоматизации и управления, готовность участвовать в разработке и изготовлении стендов для комплексной отладки и испытаний программно-аппаратных управляющих комплексов, способностью участвовать в монтаже, наладке, настройке, проверке и сдаче опытных образцов программно-аппаратных средств и комплексов автоматизации и управления).	2
10.	2	Квадрат Полибия. (готовность к участию в работах по изготовлению, отладке и сдаче в эксплуатацию систем и средств автоматизации и управления, готовность участвовать в разработке и изготовлении стендов для комплексной отладки и испытаний программно-аппаратных управляющих комплексов, способностью участвовать в монтаже, наладке, настройке, проверке и сдаче опытных образцов программно-аппаратных средств и комплексов автоматизации и управления).	1
11.	2	Таблица Виженера. (готовность к участию в работах по изготовлению, отладке и сдаче в эксплуатацию систем и средств автоматизации и управления, готовность участвовать в разработке и изготовлении стендов для комплексной отладки и испытаний программно-аппаратных управляющих комплексов, способностью участвовать в монтаже, наладке, настройке, проверке и сдаче опытных образцов программно-аппаратных средств и комплексов автоматизации и управления).	1
12.	2	Одноразовые блокноты. (готовность к участию в работах по изготовлению, отладке и сдаче в эксплуатацию систем и средств автоматизации и управления, готовность участвовать в разработке и изготовлении стендов для комплексной отладки и испытаний программно-аппаратных управляющих комплексов, способностью участвовать в монтаже, наладке, настройке, проверке и сдаче опытных образцов программно-аппаратных средств и комплексов автоматизации и управления).	2
13.	2	Разработка и изготовление стенда для комплексной отладки и испытаний программно-аппаратных управляющих комплексов защиты информации. (готовность к участию в работах по изготовлению, отладке и сдаче в эксплуатацию систем и средств автоматизации и управления, готовность участвовать в разработке и изготовлении стендов для комплексной отладки и испытаний программно-аппаратных управляющих комплексов, способностью участвовать в монтаже, наладке, настройке, проверке и сдаче опытных образцов программно-аппаратных средств и	1

		комплексов автоматизации и управления).	
14.	2	Сеть Фейштеля. Метод шифрования с открытым ключом RSA. (готовность к участию в работах по изготовлению, отладке и сдаче в эксплуатацию систем и средств автоматизации и управления, готовность участвовать в разработке и изготовлении стендов для комплексной отладки и испытаний программно-аппаратных управляющих комплексов, способностью участвовать в монтаже, наладке, настройке, проверке и сдаче опытных образцов программно-аппаратных средств и комплексов автоматизации и управления).	2
15.	2	Использование хэш-функций на примере MD5. (готовность к участию в работах по изготовлению, отладке и сдаче в эксплуатацию систем и средств автоматизации и управления, готовность участвовать в разработке и изготовлении стендов для комплексной отладки и испытаний программно-аппаратных управляющих комплексов, способностью участвовать в монтаже, наладке, настройке, проверке и сдаче опытных образцов программно-аппаратных средств и комплексов автоматизации и управления).	2
16.	2	Шифрование с открытым ключом и электронная цифровая подпись. (готовность к участию в работах по изготовлению, отладке и сдаче в эксплуатацию систем и средств автоматизации и управления, готовность участвовать в разработке и изготовлении стендов для комплексной отладки и испытаний программно-аппаратных управляющих комплексов, способностью участвовать в монтаже, наладке, настройке, проверке и сдаче опытных образцов программно-аппаратных средств и комплексов автоматизации и управления).	2
17.	3	Скрытая передача информации в изображениях. (готовность к участию в работах по изготовлению, отладке и сдаче в эксплуатацию систем и средств автоматизации и управления, готовность участвовать в разработке и изготовлении стендов для комплексной отладки и испытаний программно-аппаратных управляющих комплексов, способностью участвовать в монтаже, наладке, настройке, проверке и сдаче опытных образцов программно-аппаратных средств и комплексов автоматизации и управления).	2
18.	4	Компьютерные вирусы. (готовность к участию в работах по изготовлению, отладке и сдаче в эксплуатацию систем и средств автоматизации и управления, готовность участвовать в разработке и изготовлении стендов для комплексной отладки и испытаний программно-аппаратных управляющих комплексов, способностью участвовать в монтаже, наладке, настройке, проверке и сдаче опытных образцов программно-аппаратных средств и комплексов автоматизации и управления).	2
19.	4	Моделирование типовой атаки. (готовность к участию в работах по изготовлению, отладке и сдаче в эксплуатацию систем и средств автоматизации и управления, готовность участвовать в разработке и изготовлении стендов для комплексной отладки и испытаний программно-аппаратных управляющих комплексов, способностью участвовать в монтаже, наладке, настройке, проверке и сдаче опытных образцов программно-аппаратных средств и комплексов автоматизации и управления).	2

20.	4	Троянский конь в системе с дискреционной моделью доступа. (готовность к участию в работах по изготовлению, отладке и сдаче в эксплуатацию систем и средств автоматизации и управления, готовность участвовать в разработке и изготовлении стендов для комплексной отладки и испытаний программно-аппаратных управляющих комплексов, способностью участвовать в монтаже, наладке, настройке, проверке и сдаче опытных образцов программно-аппаратных средств и комплексов автоматизации и управления).	2
21.	4	Логические бомбы. (готовность к участию в работах по изготовлению, отладке и сдаче в эксплуатацию систем и средств автоматизации и управления, готовность участвовать в разработке и изготовлении стендов для комплексной отладки и испытаний программно-аппаратных управляющих комплексов, способностью участвовать в монтаже, наладке, настройке, проверке и сдаче опытных образцов программно-аппаратных средств и комплексов автоматизации и управления).	2
22.	4	Борьба с компьютерными вирусами с помощью диагностических утилит. (готовность к участию в работах по изготовлению, отладке и сдаче в эксплуатацию систем и средств автоматизации и управления, готовность участвовать в разработке и изготовлении стендов для комплексной отладки и испытаний программно-аппаратных управляющих комплексов, способностью участвовать в монтаже, наладке, настройке, проверке и сдаче опытных образцов программно-аппаратных средств и комплексов автоматизации и управления).	2
23.	4	Обзор антивирусных средств. Работа с антивирусными программами. (готовность к участию в работах по изготовлению, отладке и сдаче в эксплуатацию систем и средств автоматизации и управления, готовность участвовать в разработке и изготовлении стендов для комплексной отладки и испытаний программно-аппаратных управляющих комплексов, способностью участвовать в монтаже, наладке, настройке, проверке и сдаче опытных образцов программно-аппаратных средств и комплексов автоматизации и управления).	2
24.	4	Монтаж, наладка, настройка, проверка и сдача опытных образцов программно-аппаратных средств и комплексов автоматизации и управления в области защиты информации. (готовность к участию в работах по изготовлению, отладке и сдаче в эксплуатацию систем и средств автоматизации и управления, готовность участвовать в разработке и изготовлении стендов для комплексной отладки и испытаний программно-аппаратных управляющих комплексов, способностью участвовать в монтаже, наладке, настройке, проверке и сдаче опытных образцов программно-аппаратных средств и комплексов автоматизации и управления).	2
25.	5	Особенности защиты информации в устройствах, подключенных к сети Internet. (готовность к участию в работах по изготовлению, отладке и сдаче в эксплуатацию систем и средств автоматизации и управления, готовность участвовать в разработке и изготовлении стендов для комплексной отладки и испытаний программно-аппаратных управляющих комплексов, способностью участвовать в монтаже, наладке, настройке, проверке и сдаче	1

	опытных образцов программно-аппаратных средств и комплексов автоматизации и управления).	
Итого:		42

4.4 Самостоятельная работа

№ раздела	Вопросы, выносимые на самостоятельное изучение	Кол-во часов
1	2	3
1.	Средства и методы защиты информации. (готовность к участию в работах по изготовлению, отладке и сдаче в эксплуатацию систем и средств автоматизации и управления, готовность участвовать в разработке и изготовлении стендов для комплексной отладки и испытаний программно-аппаратных управляющих комплексов, способностью участвовать в монтаже, наладке, настройке, проверке и сдаче опытных образцов программно-аппаратных средств и комплексов автоматизации и управления).	15
2.	Криптография и шифрование в области защиты информации. (готовность к участию в работах по изготовлению, отладке и сдаче в эксплуатацию систем и средств автоматизации и управления, готовность участвовать в разработке и изготовлении стендов для комплексной отладки и испытаний программно-аппаратных управляющих комплексов, способностью участвовать в монтаже, наладке, настройке, проверке и сдаче опытных образцов программно-аппаратных средств и комплексов автоматизации и управления).	20
3.	Сжатие данных. (готовность к участию в работах по изготовлению, отладке и сдаче в эксплуатацию систем и средств автоматизации и управления, готовность участвовать в разработке и изготовлении стендов для комплексной отладки и испытаний программно-аппаратных управляющих комплексов, способностью участвовать в монтаже, наладке, настройке, проверке и сдаче опытных образцов программно-аппаратных средств и комплексов автоматизации и управления).	8
4.	Компьютерные вирусы. (готовность к участию в работах по изготовлению, отладке и сдаче в эксплуатацию систем и средств автоматизации и управления, готовность участвовать в разработке и изготовлении стендов для комплексной отладки и испытаний программно-аппаратных управляющих комплексов, способностью участвовать в монтаже, наладке, настройке, проверке и сдаче опытных образцов программно-аппаратных средств и комплексов автоматизации и управления).	15
5.	Правовые основы защиты информации. (готовность к участию в работах по изготовлению, отладке и сдаче в эксплуатацию систем и средств автоматизации и управления, готовность участвовать в разработке и изготовлении стендов для комплексной отладки и испытаний программно-аппаратных управляющих комплексов, способностью участвовать в монтаже, наладке, настройке, проверке и сдаче опытных образцов программно-аппаратных средств и комплексов автоматизации и управления).	3
Итого:		61

5. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

Изучение студентами дисциплины «Защита информации в технических системах» осуществляется в 7 семестре в рамках следующих организационных форм: лекции, лабораторные занятия, самостоятельная работа, контрольные мероприятия.

Достижение целей изучения дисциплины осуществляется за счет использования интерактивных образовательных технологий, которые сопровождают чтений лекционного курса по дисциплине «Защита информации в технических системах» презентацией, по всем ее разделам (выделяется на использование интерактивных образовательных технологий – 15 часов).

Применение методов ИТ – использования электронных версий учебников и учебных пособий, методических указаний (рекомендаций), и пр.

Индивидуализация обучения осуществляется за счет организации выполнения лабораторных работ каждым студентом.

Лабораторные работы направлены на закрепление теоретических знаний по вопросам защиты информации и программного обеспечения от несанкционированного доступа и копирования.

5.1 Оценочные материалы для текущего контроля успеваемости

Контрольные вопросы и задачи текущего и рубежного контроля

Контрольные мероприятия 1-ой контрольной точки

1. Лабораторные работы:
 - 1.1. Исследование возможностей системы безопасности Windows XP по разграничению полномочий пользователей.
 - 1.2. Исследование авторизации пользователей в Windows XP.
 - 1.3. Реализация дискреционной модели политики безопасности.
 - 1.4. Процедура аутентификации пользователя на основе пароля.
 - 1.5. Изучение методов парольной защиты данных.
 - 1.6. Оценка степени стойкости парольной защиты.
 - 1.7. Методы и средства защиты компьютерной информации.
2. Коллоквиум: Задания на коллоквиум по первой контрольной точке;
3. Компьютерный тестовый контроль: Банк тестовых заданий по первой контрольной точки содержит 27 заданий.

Задания на коллоквиум по первой контрольной точке

Задание №1.

1. Какова роль электропитания в защите информации?
2. Требования к комплексной системе защиты информации?
3. Термин «Информация». Что такое информация?

Задание №2.

1. защиты». Как рассредоточение и распределенность компонентов автоматических систем обработки данных обострило ситуацию с защитой информации?
2. Расскажите о простом и ограничительном условиях безопасности.
3. Раскройте термин «Физические средства защиты».

Задание №3.

1. Цель защиты информации?
2. Утечка информации по физическим каналам.
3. Раскройте термин «Организационные средства

Задание №4.

1. Какие угрозы информации автоматизированным системам обработки данных Вы можете назвать?
2. Требования к «монитору обращений». Его структура.
3. Раскройте термин «Аппаратные средства защиты».

Задание №5.

1. Перечислите и раскройте суть составляющих информационной безопасности.
2. Расскажите о развитии моделей защиты информации.
3. Раскройте термин «Программные средства защиты».

Задание №6.

1. Что понимают под заданным уровнем безопасности информации?
2. Охарактеризуйте три этапа работ по защите информации в нашей стране. Отметьте различие в подходах.
3. Авторизация. Администрирование действий пользователя.

Задание №7.

1. Риск владельца информации. Вероятность реализации угрозы и допустимость риска.
2. Методы защиты информации в автоматизированных системах.
3. Аутентификация. Определение и суть аутентификации.

Задание №8.

1. Виды ресурса, выделяемого на защиту информации.
2. Какие принципы защиты информации вы знаете?
3. Раскройте понятия инженерно-технический и программно-аппаратный элементы системы защиты информации.

Задание №9.

1. Что понимается под термином «область рациональной защиты информации»?
2. Что такое «учетная запись» в операционной системе? Ее роль.
3. Сочетания операций доступа к объекту.

Задание №10

1. Перечислите примеры опасных событий и приводящих к этому действий по отношению к защищаемой информации.
2. Чем определяется специфика уязвимостей в автоматизированных системах?
3. Три группы возможных угроз безопасности информации. Приведите примеры.

Контрольные мероприятия 2-ой контрольной точки

1. Лабораторные работы:
 - 1.1. Основы криптографической защиты информации. Шифр замены.
 - 1.2. Взлом моноалфавитного подстановочного шифра методом частотной атаки.
 - 1.3. Квадрат Полибия.
 - 1.4. Таблица Виженера.
 - 1.5. Одноразовые блокноты.
 - 1.6. Сеть Фейштеля.
 - 1.7. Метод шифрования с открытым ключом RSA.
 - 1.8. Использование хэш-функций на примере MD5.
2. Коллоквиум: Задания на коллоквиум по второй контрольной точке;
3. Компьютерный тестовый контроль: Банк тестовых заданий по второй контрольной

точке содержит 46 заданий.

Задание на коллоквиум по второй контрольной точке

Задание №1

1. Что понимается под шифрованием?
2. Расскажите об алгоритме обмена ключами Диффи-Хеллмана.
3. Что такое ключи в информационной безопасности и для чего они используются?

Задание №2

1. Что включает в себя любая криптосистема?
2. Раскройте суть шифра замены на примере «шифра Цезаря».
3. В основе каких мер безопасности лежит шифрование?

Задание №3

1. На какие типы делятся классические криптографические методы?
2. Расскажите об одноразовых блокнотах.
3. Что представляют собой основные концепции шифрования?

Задание №4

1. Какие существуют методы шифрования?
2. Что такое канальное и сквозное шифрование?
3. Приведите примеры симметричных и асимметричных шифров.

Задание №5

1. Что такое криптография? Сфера ее интересов.
2. Расскажите о подстановочных шифрах.
3. Раскройте суть шифра перестановки на примере «решетки Кардано».

Задание №6

1. Что такое аппаратное и программное шифрование?
2. Расскажите об алгоритме RSA.
3. На чем основана атака по ключам?

Задание №7

1. Каким атакам могут подвергаться системы шифрования?
2. Перечислите основные термины, связанные с шифрованием.
3. Что такое частотный анализ?

Задание №8

1. Расскажите о таблице Виженера.
2. Как происходит шифрование с использованием эллиптических кривых?
3. Чем занимается криптоанализ? Сфера его приложения.

Задание №9

1. Как происходит шифрование паролей в UNIX системах?
2. Рассказать о криптоанализе по побочным каналам.
3. Что представляет собой электронная цифровая подпись?

Задание №10

1. Что такое алгоритм DES В каких режимах может функционировать алгоритм DES?
2. Приведите примеры аппаратного шифрования.
3. В основе каких мер безопасности лежит шифрование?

Задание №11

1. Что такое шифрование с секретным ключом?
2. Сжатие и последующее шифрование. Поясните их эффективность.
3. Расскажите об отечественном стандарте шифрования «ГОСТ 28147-89».

Задание №12

1. Какие виды шифрования Вы знаете?
2. Раскройте суть процесса дешифрования.
3. Что такое криптография?

Задание №13

1. Что понимается под методом «встречи посередине»?
2. Расскажите о методе полного перебора.
3. Поясните суть правила Керкхоффа(Керкгоффса).

Задание №14

1. Что такое шифрование с открытым ключом?
2. Расскажите о алгоритме Эль-Гамала.
3. Какие методы криптоанализа Вы знаете?

Задание №15

1. Расскажите о криптоанализе хеш-функций.
2. Что представляет собой алгоритм TDES?
3. Чем определяется уровень безопасности шифросистемы

Контрольные мероприятия 3-ей контрольной точки

1. Лабораторные работы:
 - 1.1. Шифрование с открытым ключом и электронная цифровая подпись.
 - 1.2. Скрытая передача информации в изображениях.
 - 1.3. Компьютерные вирусы.
 - 1.4. Борьба с компьютерными вирусами с помощью диагностических утилит.
 - 1.5. Обзор антивирусных средств.
 - 1.6. Работа с антивирусными программами.
 - 1.7. Моделирование типовой атаки.
 - 1.8. Троянский конь в системе с дискреционной моделью доступа.
 - 1.9. Логические бомбы.
 - 1.10. Особенности защиты информации в устройствах, подключенных к сети Internet.
2. Коллоквиум: Задания на коллоквиум по третьей контрольной точке.
3. Компьютерный тестовый контроль: Банк тестовых заданий по третьей контрольной точке содержит 45 заданий.

Задания на коллоквиум по третьей контрольной точке

Задание №1

1. Роль информации в технических системах. Виды данных.
2. Криптограмма ЩНТШНЬ получена из открытого текста циклическим сдвигом букв русского алфавита (А...ДЕЖ...ЩЬ...Я) на К знаков вправо. Найдите ключ К, восстановите исходное сообщение.

Задание №2

1. Чем отличается понятие «модели безопасности» от понятия «политики безопасности»?
2. Зашифруйте текст “Системы криптографии” по шифру Цезаря, где $K = -6$.

Задание №3

1. В каких случаях применяются модели безопасности?
2. Зашифруйте текст “Средства защиты” по шифру Цезаря, где $K=2$.

Задание №4

1. Основные положения закона об информации, информационных технологиях и защите информации.
2. Зашифруйте текст “Криптографическая система” по шифру Цезаря, где $K=6$.

Задание №5

1. Основные положения закона о государственной тайне.
2. Зашифруйте текст “Системы Обработки данных” по шифру Цезаря, где $K = -2$.

Задание №6

1. Основные положения закона о защите персональных данных.
2. Зашифруйте текст “Всемирная паутина” по шифру Цезаря, где $K=3$.

Задание №7

1. Правовые средства защиты информации. Защита программных продуктов. Авторское право.
2. Зашифруйте текст “Новые технологии” по шифру Цезаря, где $K=5$.

Задание №8

1. «Политика безопасности». Основные модели «политики безопасности».
2. Расскажите о IoT и его защите.

Задание №9

1. Классификация компьютерных вирусов.
2. Зашифруйте текст “Шифр и расшифровка” по шифру Цезаря, где $K=3$.

Задание №10

1. Структура файловых, резидентных вирусов и вирусов-червей.
2. Зашифруйте текст “Аутентификация и идентификация” по шифру Цезаря, где $K=4$.

Задание №11

1. Жизненный цикл компьютерных вирусов?
1. Зашифруйте текст “Биометрические устройства” по шифру Цезаря, где $K = 4$.

Задание №12

1. Симптомы заражения вирусами. Способы заражения.
2. Дешифруйте сообщение «офмуцтфдшмг» если известно, что оно зашифровано по шифру Цезаря, с $K=3$.

Задание №13

1. Общая классификация средств защиты от вирусов
2. Правовое обеспечение защиты информации. Нормативные документы.

Задание №14

1. Основные направления компьютерных преступлений
2. Зашифруйте текст “Ассиметричные криптосистемы” по шифру Цезаря, где $K=5$.

Задание №15

1. Разрушающие программные воздействия: вирусы и закладки.
2. С помощью ключа УСТРОЙСТВО зашифруйте словосочетание «информация, как средство познания мира».

ТЕСТЫ:

F1: Защита информации в технических системах для 4 курса бакалавриата УТС, 7 сем

F2: Шаповалов В. А.

V1: Средства и методы защиты информации (1 рейтинговая точка)

V2: Основные понятия и определения

I: 1

S: Как называется умышленно искаженная информация?

+: Дезинформация

- : Информативный поток
- : Достоверная информация
- : Перестает быть информацией

I: 2

S: Как называется информация, к которой ограничен доступ?

- +: Конфиденциальная
- : Противозаконная
- : Открытая
- : Недоступная

I: 3

S: Что называют защитой информации?

- : Называют деятельность по предотвращению утечки защищаемой информации
- : Называют деятельность по предотвращению несанкционированных воздействий на защищаемую информацию
- : Называют деятельность по предотвращению непреднамеренных воздействий на защищаемую информацию
- +: Все ответы верны

I: 4

S: Под непреднамеренным воздействием на защищаемую информацию понимают?

- +: Воздействие на нее из-за ошибок пользователя, сбоя технических или программных средств и воздействие природных явлений
- : Процесс ее преобразования, при котором содержание информации изменяется на ложную
- : Возможности ее преобразования, при котором содержание информации изменяется на ложную информацию
- : Некоторые ограничения доступа в отдельные отрасли экономики или на конкретные производства

I: 5

S: Элемент аппаратной защиты, где используется установка источников бесперебойного питания (UPS)?

- +: защита от сбоев в электропитании
- : защита от сбоев серверов, рабочих станций и локальных компьютеров

- : защита от сбоев устройств для хранения информации
- : защита от утечек информации электромагнитных излучений

I: 6

S: Функция защиты технической системы, гарантирующая то, что доступ к информации, хранящейся в системе может быть осуществлен только тем лицам, которые на это имеют право

- +: управление доступом
- : аутентичность
- : целостность
- : доступность

I: 7

S: ### - это гарантия сохранности данными правильных значений, которая обеспечивается запретом для неавторизованных пользователей каким-либо образом модифицировать, разрушать или создавать данные.

- +: целостность

I: 8

S: Предоставление легальным пользователям дифференцированных прав доступа к ресурсам системы – это ###

- +: авторизация

I: 9

S: Присвоение субъектам и объектам доступа уникального номера, шифра, кода и т.п. с целью получения доступа к информации – это ###

- +: идентификация

I: 10

S: Проверка подлинности пользователя по предъявленному им идентификатору – это ###

- +: аутентификация

I: 11

S: Свойство, которое гарантирует, что информация не может быть доступна или раскрыта для неавторизованных личностей, объектов или процессов – это ###

- +: конфиденциальность

I: 12

S: В многоуровневой модели, если субъект доступа формирует запрос на изменение, то уровень безопасности объекта относительно уровня безопасности субъекта должен ###

+: доминировать

I: 13

S: В многоуровневой модели, если субъект доступа формирует запрос на чтение-запись, то уровень безопасности субъекта относительно уровня безопасности объекта должен ###

+: быть равен

I: 14

S: В многоуровневой модели, если субъект доступа формирует запрос на чтение, то уровень безопасности субъекта относительно уровня безопасности объекта должен ###

+: доминировать

I: 15

S: Возможность получения необходимых пользователю данных или сервисов за разумное время характеризует свойство ###

+: доступность

I: 16

S: Восстановление данных является дополнительной функцией следующей услуги защиты - ###

+: целостность

I: 17

S: Защита информации, определяющей конфигурацию системы, является основной задачей средств защиты ### в ОС

+: встроенных

-: учитываемых

-: установленных извне

I: 18

S: Аутентификация используется на уровнях:

-: прикладном

- : сетевом
- : транспортном
- +: всех перечисленных

I: 19

S: Базовыми услугами для обеспечения безопасности компьютерных систем и сетей являются:

- : аутентификация
- : контроль доступа
- : причастность
- : целостность
- +: все приведенные

I: 20

S: В автоматизированных системах используется аутентификация по:

- : паролю
- : предмету
- : физиологическим признакам
- +: возможна по всем перечисленным

I: 21

S: В обязанности сотрудников группы информационной безопасности входят:

- : расследование причин нарушения защиты
- : управление доступом пользователей к данным
- +: все перечисленное

I: 22

S: В файловых системах ОС UNIX права доступа к файлу определяются для:

- : владельца
- : всех основных пользователей
- : членов группы владельца
- +: всех перечисленных вариантов

I: 23

S: Для аутентификации по физиологическим признакам терминальных пользователей

наиболее приемлемыми считаются:

- : голос
- : личная подпись
- : отпечатки пальцев
- : форма кисти
- +: все перечисленное

I: 24

S: Для разграничения доступа к файлу применяются флаги, разрешающие:

- : выполнение
- : запись
- : чтение
- +: все перечисленное

I: 25

S: Защита процедур и программ осуществляется на уровнях:

- : аппаратуры
- : данных
- : программного обеспечения
- +: всех перечисленных

I: 26

S: Структура ОС с точки зрения анализа ее безопасности включает уровни:

- : внешний
- : приложений
- : сетевой
- : системный
- +: все перечисленные

I: 27

S: Функция подтверждения подлинности сообщения НЕ использует следующее:

- : доставка по адресу
- +: санкционированный канал связи
- : неизменность сообщения при передаче
- : санкционированный отправитель

V1: Криптография и шифрование в области защиты информации (2 рейтинговая точка)

V2: Основы криптографии. Методы и стандарты шифрования данных в вычислительных системах. Сжатие данных как способ кодирования.

I: 1

S: Шифрование информации это

- + : Процесс ее преобразования, при котором содержание информации становится непонятным для не обладающих соответствующими полномочиями субъектов
- : Процесс преобразования, при котором информация удаляется
- : Процесс ее преобразования, при котором содержание информации изменяется на ложную
- : Процесс преобразования информации в машинный код

I: 2

S: Наука которая занимается обеспечением скрытности информации в информационных массивах за счет сокращения и уплотнения (например, текста).

- + : стенография
- : стеганография
- : криптоанализ
- : криптография

I: 3

S: Как называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения.

- : личной подписью
- : идентификатором
- + : электронной подписью
- : QR-кодом

I: 4

S: Как называется удачная криптоатака?

- + : взломом
- : серфингом
- : баффингом
- : подключением

I: 5

S: Что такое несанкционированный доступ?

- + : Доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа
- : Создание резервных копий в организации
- : Вход в систему без согласования с руководителем организации
- : Удаление не нужной информации

I: 6

S: Цифровая подпись используется для обеспечения услуг:

- + : аутентификации
- : контроля доступа
- : контроля трафика
- + : целостности

I: 7

S: Что такое симметричный метод шифрования?

- + : Криптографический метод защиты информации, где для шифрования и дешифрования используется один и тот же ключ, сохранение которого в секрете обеспечивает надежность защиты
- : Метод защиты информации, где для шифрования используется открытый ключ, для дешифрования используется закрытый ключ
- : Преобразование, которое позволяет пользователям проверить авторство и подлинность
- : Метод защиты информации, где шифрование и дешифрование производят набором симметричных ключей

I: 8

S: Какие методы применяются в простейших криптографических методах защиты информации?

- + : Подстановка и Перестановка
- : Аналитическое преобразование
- : Комбинированное преобразование
- : Замена контрольными суммами
- : Замена только цифр

I: 9

S: Что такое асимметричный метод шифрования?

- + : Метод защиты информации, где для шифрования и дешифрования информации используются различные ключи
- : Метод защиты информации, где для шифрования и дешифрования информации используются больше трех ключей
- : Метод защиты информации, где для шифрования и дешифрования информации используют астрономические методы
- : Метод защиты информации, где шифрование и дешифрование информации осуществляют без ключа

I: 10

S: Что такое закрытый ключ электронной цифровой подписи?

- + : Уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи.
- : Ключ электронной цифровой подписи, который зашифрован с помощью единственного симметричного ключа владельца
- : Ключ электронной цифровой подписи, который хранится отдельно от других закрытый ключей
- : Ключ электронной цифровой подписи, которым шифруют заголовки электронных документов для установления подлинности владельца

I: 12

S: Обеспечением скрытности информации в информационных массивах занимается

- : криптография
- : криптоанализ
- : криптология
- + : стеганография

I: 13

S: Многоалфавитным шифром замены является:

- : шифр Цезаря
- + : таблица Виженера
- : квадрат Полибия

-: считаль Лесандра

I: 14

S: К шифрам перестановки относится:

+: решетка Кардано

-: шифр Плейфера

-: шифр Грансфельда

-: шифр Цезаря

I: 15

S: Основное средство, обеспечивающее конфиденциальность информации, посылаемой по открытым каналам передачи данных:

-: Идентификация

-: Аутентификация

-: Авторизация

+: Шифрование

I: 16

S: Что такое Хэш-функция?

+: Труднообратимое преобразование данных (односторонняя функция), реализуемое, как правило, средствами симметричного шифрования со связыванием блоков

-: Уникальный метод шифрования и дешифрования информации

-: Выполнение предварительных операций перед шифрованием и дешифрованием

-: Функция распределения файлов по названиям и принадлежности к определенным документам

I: 17

S: Частотный анализ шифра позволяет:

-: определить число вхождений символа алфавита в текст

-: определить число букв сообщения

+: дешифровать сообщение, учитывая показатели частоты встречаемости

-: осуществить атаку на сервер

I: 18

S: С помощью закрытого ключа информация

- : копируется
- : транслируется
- +: расшифровывается
- : зашифровывается

I: 20

S:### занимается обеспечением скрытности информации в информационных массивах за счет сокращения и уплотнения (например, текста).

- +: стенография

I: 21

S: ### называется конечное множество используемых для кодирования информации знаков.

- +: алфавитом

I: 22

S: ### называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения.

- +: электронной подписью

I: 23

S: ### объединяет математические методы нарушения конфиденциальности и аутентичности информации без знания ключей.

- +: криптоанализ

I: 24

S: ### является наиболее надежным механизмом для защиты содержания сообщений.

- +: криптография

I: 25

S: ### является наукой, изучающей математические методы защиты информации путем ее преобразования.

- +: криптология

I: 26

S: Показатель ### является главным параметром криптосистемы.

+: криптостойкости

I: 27

S: Два ключа используются в криптосистемах

+: с открытым ключом

-: с закрытым ключом

-: с симметричным шифрованием

-: с простой заменой

I: 28

S: Длина исходного ключа в ГОСТ 28147-89 (бит)

-: 250

-: 245

+: 256

-: 278

I: 29

S: ГОСТ 28147-89 используется в режимах:

-: электронная кодированная книга

+: гаммирование

-: простая замена с обратной связью

+: простая замена

I: 30

S: Криптография НЕ включает:

-: криптосистемы с открытым ключом

-: симметричные криптосистемы

+: асимметричные криптосистемы

-: системы электронной подписи

I: 31

S: Безопасная система НЕ обладает свойством:

-: доступность

- : конфиденциальность
- : целостность
- +: восстанавливаемость

I: 32

S: Подсистема управления криптографическими ключами структурно состоит из:

- : программно-аппаратных средств
- : центра распределения ключей
- +: всего перечисленного

I: 33

S: Угрозы безопасности по предпосылкам появления классифицируются как:

- +: объективная и субъективная
- : преднамеренная и случайная
- : гипотетическая и реальная

I: 34

S: Угрозы безопасности по природе происхождения классифицируются как:

- : объективная и субъективная
- +: преднамеренная и случайная
- : гипотетическая и реальная

I: 35

S: Наименее затратный криптоанализ для криптоалгоритма DES

- : перебор по выборочному ключевому пространству
- : разложение числа на сложные множители
- +: перебор по всему ключевому пространству
- : разложение числа на простые множители

I: 36

S: Недостаток систем шифрования с открытым ключом

- : при использовании простой замены легко произвести подмену одного шифрованного текста другим
- +: относительно низкая производительность
- : необходимость распространения секретных ключей

-: на одном и том же ключе одинаковые 64-битные блоки открытого текста перейдут в одинаковые блоки шифрованного текста

I: 37

S: Информация, переданная или полученная пользователем информационно-телекоммуникационной сети:

+: Электронное сообщение

-: Информационное сообщение

-: Текстовое сообщение

-: Визуальное сообщение

I: 38

S: Основное средство, обеспечивающее конфиденциальность информации, посылаемой по открытым каналам передачи данных:

-: Идентификация

-: Аутентификация

-: Авторизация

+: Шифрование

I: 39

S: К биометрической системе защиты относятся:

-: Защита паролем

-: Антивирусная защита

+: Идентификация по радужной оболочке глаз

+: Идентификация по отпечаткам пальцев

I: 40

S: Присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения, называется

+: электронной подписью

-: шифром

-: ключом

-: идентификатором

I: 41

S:Правило, суть которого состоит в том, что при построении криптографической системы предполагается, что противнику известен алгоритм шифрования

- + : правило Керкгоффа
- : правило Крюгера
- : правило Золингера
- : правило Шредера

I: 42

S:Криптографические методы защиты информации применяются в следующих прикладных задачах:

- : электронная цифровая подпись
- : электронные деньги
- : электронное голосование
- : защита ценных бумаг и документов
- + : во всех перечисленных

I: 43

S: В перечень требований к системам шифрования не входит:

- : наличие нескольких ключей
- + : нераскрываемость
- : компрометация системы не причиняет неудобств пользователям

I: 44

S:В криптографические принципы НЕ входит:

- : рассеивание
- : перемешивание
- + : повторение
- : перестановка

I: 45

S:Какие операции предполагает шифрованная связь?

- + : шифрование
- + : расшифровывание
- : взлом

-: хищение

I: 46

S: К криптоалгоритмам с открытым ключом НЕ относится:

-: криптосистема RSA

-: криптосистема Эль-Гамала (EGCS)

-: криптосистема на эллиптических кривых (ECCS)

+: криптосистема RC5

V1: Вредоносные программы, средства борьбы с ними и правовые основы защиты информации (3 рейтинговая точка)

V2: Компьютерные вирусы. Антивирусные средства. Применение патентования и норм авторского права при защите программных продуктов. Основные положения Закона об охране программ для ЭВМ и баз данных.

I: 1

S: Аспектами адекватности средств защиты являются:

+: корректность

-: конфиденциальность

+: эффективность

I: 2

S: Видами политики безопасности являются:

-: оптимальная

-: минимальная

+: избирательная

+: полномочная

I: 3

S: Группами требований к документированию системы защиты информации являются:

+: обработка угроз

+: протоколирование

+: тестирование программ

-: аутентификация

I: 4

S: Подсистема регистрации и учета системы защиты информации должна обеспечивать:

- + : оповещение о попытках нарушения защиты
- + : учет носителей информации
- : подтверждение получения сообщения
- : управление потоками информации

I: 5

S: Подсистема управления доступом системы защиты информации должна обеспечивать:

- + : аутентификация
- + : идентификация
- + : управление потоками информации
- : учет носителей информации

I: 6

S: Процесс анализа рисков при разработке системы защиты ИС включает:

- + : анализ потенциальных угроз
- + : оценка возможных потерь
- : анализ потенциального злоумышленника

I: 7

S: Различают модели воздействия программных закладок на компьютеры:

- : искажение
- : наблюдение и компрометация
- : перехват
- : уборка мусора
- + : все перечисленные

I: 8

S: Субъектами для монитора обращений НЕ являются:

- : порты
- : программы
- : терминалы
- + : файлы

I: 9

S: Объектами для монитора обращений являются:

- + : задания
- : терминалы
- : порты
- + : файлы

I: 10

S: Составляющими информационной базы для монитора обращений являются:

- + : виды доступа
- : программы
- : нормы

I: 11

S: По методу внедрения в компьютерную систему различают:

- : вирусные
- : троянские
- + : программно-аппаратные
- + : драйверные

I: 12

S: Все клавиатурные шпионы делятся на:

- : перехватчики
- + : имитаторы
- : наблюдатели
- + : фильтры

I: 13

S: Основной документ, на основе которого проводится политика информационной безопасности?

- + : программа информационной безопасности
- : регламент информационной безопасности
- : политическая информационная безопасность
- : протекторат

I: 14

S: Основные предметные направления Защиты Информации?

- + : охрана государственной, коммерческой, служебной, банковской тайн, персональных данных и интеллектуальной собственности
- : Охрана золотого фонда страны
- : Определение ценности информации
- : Усовершенствование скорости передачи информации

I: 15

S: Государственная тайна это

- + : защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны
- : ограничения доступа в отдельные отрасли экономики или на конкретные производства
- : защищаемые банками и иными кредитными организациями сведения о банковских операциях
- : защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

I: 16

S: Коммерческая тайна это....

- : защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны
- + : ограничения доступа в отдельные отрасли экономики или на конкретные производства
- : защищаемые банками и иными кредитными организациями сведения о банковских операциях
- : защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

I: 17

S: Путь несанкционированного распространения носителя информации от источника к злоумышленнику называется ### утечки информации

- + : каналом

I: 18

S: ### называется получение и анализ информации о состоянии ресурсов системы с помощью специальных средств контроля.

+: мониторингом

I: 19

S: Действие программных закладок основывается на инициировании или подавлении сигнала о возникновении ошибочных ситуаций в компьютере в рамках модели ###

+: искажение

I: 20

S: Часть программы с известными пользователю функциями, способная выполнять действия с целью причинения определенного ущерба – это ###

+: троянские программы

I: 21

S: ### называется нормативный документ, регламентирующий все аспекты безопасности продукта информационных технологий.

+: профилем защиты

I: 22

S: Если средства защиты могут быть преодолены только государственной спецслужбой, то согласно "Европейским критериям" безопасность считается ###

+: высокой

I: 23

S: Если средство защиты способно противостоять корпоративному злоумышленнику, то согласно "Европейским критериям" безопасность считается ###

+: средней

I: 24

S: Если средство защиты способно противостоять отдельным атакам, то согласно "Европейским критериям" безопасность считается ###

+: базовой

I: 25

S: В модели политики безопасности Лендвера сущностью могут являться:

+: контейнер

+: объект

-: множество

-: операция

I: 26

S: Согласно "Оранжевой книге" требованиями в области аудита являются:

+: идентификация и аутентификация

-: политика безопасности

-: корректность

+: регистрация и учет

I: 27

S: Из перечисленных моделей: 1) Адепт-50; 2) игровая; 3) Хартстона; 4) с полным перекрытием; 5) Белла-ЛаПадула; 6) LWM – моделями политики безопасности на основе анализа угроз системе являются

+: 2, 4

-: 1, 3

-: 1, 5, 6

-: 1, 2, 3

I: 28

S: Из перечисленных уровней безопасности: 1) базовый; 2) низкий; 3) средний; 4) стандартный; 5) высокий – в "Европейских критериях" определены

+: 1, 3, 5

-: 2, 3, 4

-: 1, 4

-: 2, 5

I:

S: Вредоносная программа, которая подменяет собой загрузку некоторых программ при загрузке системы называется...

+: Загрузочный вирус

- : Макровирус
- : Троян
- : Сетевой червь
- : Файловый вирус

I: 29

S: Компьютерные вирусы это

- : Вредоносные программы, наносящие вред данным.
- : Программы, уничтожающие данные на жестком диске
- +: Программы, которые могут размножаться, и скрыто внедрять свои копии в файлы, загрузочные сектора дисков, документы.
- : Программы, заражающие загрузочный сектор дисков и препятствующие загрузке компьютера
- : Это скрипты, помещенные на зараженных интернет – страничках

I: 30

S: Вредоносные программы - это

- : шпионские программы
- +: программы, наносящие вред данным и программам, находящимся на компьютере
- : антивирусные программы
- : программы, наносящие вред пользователю, работающему на зараженном компьютере

I: 31

S: Какое определение информации дано в Законе РФ "Об информации, информатизации и защите информации"?

- +: Сведения о лицах, предметах, фактах, событиях, явлениях и процессах, независимо от формы их представления
- : Получение сведений из глобальной информационной сети
- : Систематизированные данные об экономике
- : Это результаты компьютерных решений определенных задач

I: 32

S: Что относится к правовым мерам защиты информации?

- +: Законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения

- : Действия правоохранительных органов для защиты информационных ресурсов
- : Организационно-административные меры для защиты информационных ресурсов
- : Действия администраторов сети защиты информационных ресурсов

I: 33

S: Какими способами обеспечиваются основные уровни антивирусной защиты?

- + :Поиск и уничтожение известных вирусов
- + : Поиск и уничтожение неизвестных вирусов
- + : Блокировка проявления вирусов
- : Определения адреса отправителя вирусов
- : Выявление создателей вирусов

I: 34

S: Какие имеются методы и средства поиска и уничтожения известных вирусов?

- + :Метод сканирования и сравнения с уникальным фрагментом программного кода, находящимся в базе данных кодов известных компьютерных вирусов.
- : Метод проведения математических вычислений по заранее известным алгоритмам
- : Метод сравнения количества значений равных 0 с количеством значений равных 1
- : Метод сравнения контрольных служебных значений файлов

I: 35

S: Какие имеются методы и средства поиска и уничтожения неизвестных вирусов

- + :Метод контроля целостности системы (обнаружение изменений)
- : Метод проведения математических вычислений по заранее известным алгоритмам
- : Метод выявления создателей вирусов
- : Метод проверки наличия служебных символов в файле

I: 36

S: На каких методах основана блокировка проявления вирусов?

- + :На методах перехвата характерных для вирусов функций
- : На методах вероятностного проявления кодов разрушения файлов
- : На методах проверок и сравнениях с контрольной копией

I: 37

S: Программный модуль, который имитирует приглашение пользователю

зарегистрироваться для того, чтобы войти в систему, является клавиатурным шпионом типа

-: фильтр

-: заместитель

-: перехватчик

+:имитатор

I: 38

S: Формирование политики безопасности организации относится к:

+:организационным мерам обеспечения безопасности

-: техническим мерам обеспечения безопасности

-: морально-этическим мерам обеспечения безопасности

-: правовым мерам обеспечения безопасности

I: 39

S: Установка аппаратного межсетевого экрана относится к:

+:техническим мерам обеспечения безопасности

-: морально-этическим мерам обеспечения безопасности

-: физическим мерам обеспечения безопасности

-: организационным мерам обеспечения безопасности

I: 40

S: Как называется состояние защищенности личности, общества и государства от внутренних и внешних угроз, которое позволяет обеспечить конституционные права, свободы, достойные качество и уровень жизни граждан, суверенитет, территориальную целостность и устойчивое развитие Российской Федерации, оборону и безопасность государства?

-: информационная безопасность

-: государственная безопасность

+:национальная безопасность

-: общественная безопасность

I: 41

S: Как называется модель нарушителя, которая отражает систему принятых руководством объекта защиты взглядов на контингент потенциальных нарушителей, причины и мотивацию их действий, преследуемые цели и общий характер действий в процессе

подготовки и совершения акций воздействия?

- : косвенная
- : количественная
- +:содержательная
- : математическая

I: 42

S: Как называется доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами?

- : дискреционный доступ
- : атака
- : мандатный доступ
- +:несанкционированный доступ

I: 43

S: Позволяет получать доступ к информации, перехваченной другими программными закладками, модель воздействия программных закладок типа

- : перехват
- +:уборка мусора
- : наблюдение
- : компрометация

I: 44

S: Первым этапом разработки системы защиты ИС является

- +:анализ потенциально возможных угроз информации
- : изучение информационных потоков
- : стандартизация программного обеспечения
- : оценка возможных потерь

I: 45

S: Цель процесса внедрения и тестирования средств защиты —

- : определить уровень расходов на систему защиты
- : выявить нарушителя
- +: гарантировать правильность реализации средств защиты

-: выбор мер и средств защиты

Примерные темы рефератов на выбор

1. Техническая защита информации. Основные технологии построения защищенных информационных систем
2. Политика безопасности. Критерии и классы защищенности средств вычислительной техники и автоматизированных систем.
3. Защита информации при реализации информационных процессов (ввод, вывод, передача, обработка, накопление, хранение).
4. Классификация информации. Виды данных и носителей.
5. Виды защищаемой информации. Ценность информации. Цена информации.
6. Демаскирующие признаки объектов защиты.
7. Классификация источников и носителей информации.
8. Способы наблюдения с использованием технических средств.
9. Каналы утечки информации. Технические каналы утечки. Активные и пассивные методы защиты информации от утечки по техническим каналам.
10. Классификация технических каналов утечки по времени функционирования, структуре, информативности, физической природе носителя.
11. Видеоконтроль, телевизионные системы наблюдения. Наблюдение в оптическом диапазоне и применяемые для этого средства.
12. Перехват электромагнитных излучений.
13. Акустическое подслушивание. Эффекты, возникающие при подслушивании.
14. Криптографическая защита информации.
15. Методы шифрования данных.
16. Стандарт шифрования данных DES. Использование ключей и цифровых подписей.
17. Стойкость алгоритмов шифрования. Типы алгоритмов шифрования. Примеры криптографических алгоритмов.
18. Методы обеспечения достоверности передачи информации.
19. Понятие разрушающего программного воздействия. Методы перехвата и навязывания информации. Компьютерные вирусы. Понятия о видах вирусов.
20. Классификация современных антивирусных программ.
21. Системный подход к защите информации. Этапы разработки мер по предотвращению угроз утечки информации.
22. Состав инженерной защиты и технической охраны объектов.
23. Инженерные конструкции и сооружения для защиты информации. Их классификация.

24. Средства идентификации личности. Защита личности как носителя информации.
25. Классификация датчиков охранной сигнализации и извещателей.

5.2. Оценочные материалы для промежуточной аттестации

Промежуточная аттестация проходит в форме экзамена в 7 семестре ОФО. На экзамене студенту предлагается ответить на теоретические вопросы. Экзаменационный билет включает три теоретических вопроса.

Вопросы к экзамену

1. Основные положения закона об информации, информационных технологиях и защите информации.
2. Понятие государственной тайны. Основные положения закона о государственной тайне.
3. Основные положения закона о защите персональных данных.
4. Значение защиты информации. Цель и принципы защиты. Анализ схем защиты.
5. Средства опознавания и разграничения доступа к информации.
6. Основные каналы утечки информации. Защита от утечки информации по техническим каналам.
7. Методы и средства защиты информации. Содержание способов и средств обеспечения безопасности информации.
8. Обзор и классификация методов шифрования информации.
9. Защита информации в процессе изготовления, отладки и сдачи в эксплуатацию систем и средств автоматизации и управления.
10. Дайте характеристику шифра DES. Опишите причину его замены на TDES.
11. Дайте характеристику шифра ГОСТ 28147-89.
12. Поточное и блочное шифрование. Их отличие. Режим применения блочного шифра.
13. Хэш-функции. Основные свойства и принципы работы.
14. Отличие криптографии с открытым ключом от симметричных шифров.
15. Опишите алгоритм Диффи-Хеллмана. Его протокол.
16. Опишите алгоритм Эль-Гамала. Его использование в цифровой подписи.
17. Опишите алгоритм RSA. Его использование в цифровой подписи.
18. Опишите алгоритм ECC. Сферы его применения.
19. Аутентификация и идентификация, их отличия. Устройства идентификации и аутентификации.
20. Принципы использования многофакторных паролей.

21. Получение одноразовых паролей.
22. Криптография и криптоанализ. Сфера их интересов. Применение криптографии.
23. Криптография. Симметричные криптосистемы.
24. Криптография. Асимметричные криптосистемы
25. Криптосистемы. Отличие симметричной и асимметричной криптосистем.
26. Криптосистемы и их классификация.
27. Шифрование. Виды и методы шифрования. Меры безопасности.
28. Шифрование с открытым ключом.
29. Шифрование с секретным ключом.
30. Процесс дешифрования.
31. Шифрование информации станций для комплексной отладки и испытаний программно-аппаратных управляющих комплексов.
32. Шифр перестановки на примере «решетки Кардано».
33. Ключи и их использование. Атака по ключам.
34. Компьютерные вирусы. Классификация компьютерных вирусов.
35. Структура файловых, резидентных вирусов и вирусов-червей.
36. Компьютерные вирусы. Жизненный цикл компьютерных вирусов.
37. Компьютерные вирусы. Способы и симптомы заражения вирусами.
38. Компьютерные вирусы. Общая классификация средств защиты от вирусов.
39. Основные направления компьютерных преступлений.
40. Логическая бомба. Ее внедрение в ОС или ПО. Разрушающие программные воздействия: вирусы и закладки.
41. Средства защиты информации. Антивирусные средства (Сканеры, Мониторы, Ревизоры, Блокировщики, Иммунизаторы).
42. Монтаж, наладка, настройка, проверка и сдача опытных образцов программно-аппаратных средств и комплексов автоматизации и управления защиты информации.
43. Правовые средства защиты информации. Защита программных продуктов. Авторское право.
44. Виды противников или «нарушителей». Понятие о видах вирусов.
45. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
46. Использование защищенных компьютерных систем.
47. Методы криптографии.
48. Технологии построения защищенных систем.
49. Технические аспекты обеспечения защиты информации. Современное состояние

50. Правовые основы защиты информации.
51. Криптоанализ. Современные криптографические системы.
52. Современные средства защиты информации.
53. Требования предъявляемые к автоматизированным системам в области защиты информации.
54. Сущность линейного криптоанализа.
55. Дифференциальный криптоанализ.
56. Классификация криптографических алгоритмов по стойкости.
57. Анализ надежности криптосистем.
58. Схемы аутентификации.
59. Требования к экранированию помещений, предназначенных для размещения вычислительной техники.
60. Информационно-опасные сигналы, их основные параметры.

6. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности.

6.1 Результаты освоения учебной дисциплины, подлежащие проверке.

Шифр компетенции	Компетенция	Показатели оценивания компетенций	Критерии оценивания компетенций
1	2	3	4
ПК-10	готовность к участию в работах по изготовлению, отладке и сдаче в эксплуатацию систем и средств автоматизации и управления.	В ходе текущего, рубежного контроля, лабораторных работ показать способность к участию в работах по изготовлению, отладке и сдаче в эксплуатацию систем и средств автоматизации и управления.	Наличие показателя – удовлетворительно; Наличие перспектив развития проекта или обозначены перспективы развития в составе последующих проектов - хорошо; Уровень проекта, предполагающий проработку использование как отдельного модуля в проектах других студентов - отлично.
ПК-13	готовность участвовать в разработке и изготовлении стендов для комплексной отладки и испытаний программно-аппаратных управляющих комплексов.	В ходе текущего, рубежного контроля, лабораторных работ показать готовность участвовать в разработке и изготовлении стендов для комплексной отладки и испытаний программно-аппаратных управляющих комплексов.	Наличие показателя – удовлетворительно; Наличие перспектив развития проекта или обозначены перспективы развития в составе последующих проектов - хорошо; Уровень проекта, предполагающий проработку использование как отдельного модуля в проектах других студентов - отлично.

ПК-14	способностью участвовать в монтаже, наладке, настройке, проверке и сдаче опытных образцов программно-аппаратных средств и комплексов автоматизации и управления.	В ходе текущего, рубежного контроля, лабораторных работ показать способность к разработке и использованию испытательных стендов на базе современных средств вычислительной техники и информационных технологий для комплексной отладки, испытаний и сдачи в эксплуатацию систем управления.	Наличие показателя – удовлетворительно; Наличие перспектив развития проекта или обозначены перспективы развития в составе последующих проектов - хорошо; Уровень проекта, предполагающий проработку использование как отдельного модуля в проектах других студентов - отлично.
--------------	--	---	--

Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Результаты обучения (объекты оценивания)	Основные показатели оценки результатов	Оценочные средства
1	2	3
З1 Знать теоретические составляющие защиты информации.	- описание основ; - выполнение тестов; - выполнение и защита лабораторных работ	лабораторная работа, контрольная работа, коллоквиум, защита реферата, тестирование, экзамен
У1 Уметь выявлять источники, риски и формы атак на информацию.	- описание основ; - выполнение тестов; - выполнение и защита лабораторных работ	лабораторная работа, контрольная работа коллоквиум, защита реферата, тестирование, экзамен
У2 Уметь работать в соответствии со стандартами безопасности.	- описание основ; - выполнение тестов; - выполнение и защита лабораторных работ	лабораторная работа, контрольная работа коллоквиум, защита реферата, тестирование, экзамен
У3 Уметь использовать криптографические модели, алгоритмы шифрования информации и аутентификации пользователей.	- описание основ; - выполнение тестов; - выполнение и защита лабораторных работ	лабораторная работа, контрольная работа коллоквиум, защита реферата, тестирование, экзамен
У4 Уметь составлять многоуровневую защиту данных.	- описание основ; - выполнение тестов; - выполнение и защита лабораторных работ	лабораторная работа, контрольная работа коллоквиум, защита реферата, тестирование, экзамен
В1 Владеть навыками проектирования систем защиты информации.	- описание основ; - выполнение тестов; - выполнение и защита лабораторных работ	лабораторная работа, контрольная работа коллоквиум, защита реферата, тестирование, экзамен

6.2 Шкала оценивания планируемых результатов обучения

Текущий и рубежный контроль

В рамках текущего и рубежного контроля по дисциплине студент может набрать до 70 баллов:

Семестр	Шкала оценивания			
	0-35 баллов	36-50 баллов	51-60 баллов	61-70 баллов
7	Частичное посещение аудиторных занятий. Неудовлетворительное выполнение лабораторных и практических работ. Плохая подготовка к балльно-рейтинговым мероприятиям. Студент не допускается к промежуточной аттестации	Полное или частичное посещение аудиторных занятий. Частичное выполнение и защита лабораторных и практических работ. Выполнение контрольных работ, тестовых заданий на оценки «удовлетворительно».	Полное или частичное посещение аудиторных занятий. Полное выполнение и защита лабораторных и практических работ. Выполнение контрольных работ, тестовых заданий на оценки «хорошо».	Полное посещение аудиторных занятий. Полное выполнение и защита лабораторных и практических занятий. Выполнение контрольных работ, тестовых заданий на оценки «отлично».

Промежуточная аттестация.

Оценка результатов освоения учебной дисциплины в 7 семестре проводится по шкале, используемой на экзамене:

Семестр	Шкала оценивания			
	Неудовлетворительно (36-60 баллов)	Удовлетворительно (61-80 баллов)	Хорошо (81-90 баллов)	Отлично (91-100 баллов)
7	Студент имеет 36-60 баллов по итогам текущего и рубежного контроля, на экзамене не дал полного ответа ни на один вопрос. Студент имеет 36-45 баллов по итогам текущего и рубежного контроля, на экзамене дал полный ответ только на один вопрос	Студент имеет 36-50 баллов по итогам текущего и рубежного контроля, на экзамене дал полный ответ на один вопрос и частично (полностью) ответил на второй. Студент имеет 46-60 баллов по итогам текущего и рубежного контроля, на экзамене дал полный ответ на один вопрос или частично ответил на оба вопроса. Студент имеет по итогам текущего и	Студент имеет 51-60 баллов по итогам текущего и рубежного контроля, на экзамене дал полный ответ на один вопрос и частично (полностью) ответил на второй. Студент имеет 61 – 65 баллов по итогам текущего и рубежного контроля, на экзамене дал полный ответ на один вопрос и частично ответил	Студент имеет 61-70 баллов по итогам текущего и рубежного контроля, на экзамене дал полный ответ на один вопрос и частично (полностью) ответил на второй.

		рубежного контроля 61-70 баллов на экзамене не дал полного ответа ни на один вопрос.	на второй. Студент имеет 66-70 баллов по итогам текущего и рубежного контроля, на экзамене) дал полный ответ только на один вопрос.	
--	--	--	---	--

7. Учебно-методическое обеспечение дисциплины

7.1. Основная литература

1. Астайкин А.И. и др. Методы и средства обеспечения программно-аппаратной защиты информации [Электронный ресурс]: научно-техническое издание — Электрон. текстовые данные.— Саратов: Российский федеральный ядерный центр – ВНИИЭФ, 2015.— 224 с.— Режим доступа: <http://www.iprbookshop.ru/60959.html>.
2. Голиков А.М. Защита информации от утечки по техническим каналам [Электронный ресурс]: учебное пособие — Электрон. текстовые данные.— Томск: Томский государственный университет систем управления и радиоэлектроники, 2015.— 256 с.— Режим доступа: <http://www.iprbookshop.ru/72090.html>.
3. Камский В.А. Защита личной информации в Интернете, смартфоне и компьютере [Электронный ресурс]/ Камский В.А.— Электрон. текстовые данные.— СПб.: Наука и Техника, 2017.— 272 с.— Режим доступа: <http://www.iprbookshop.ru/73046.html>.
4. Кирпичников А.П., Хайбуллина З.М. Криптографические методы защиты компьютерной информации [Электронный ресурс]: учебное пособие — Электрон. текстовые данные.— Казань: Казанский национальный исследовательский технологический университет, 2016.— 100 с.— Режим доступа: <http://www.iprbookshop.ru/79313.html>.
5. Краковский Ю.М. Защита информации [Электронный ресурс]: учебное пособие/ Краковский Ю.М.— Электрон. текстовые данные.— Ростов-на-Дону: Феникс, 2016.— 349 с.— Режим доступа: <http://www.iprbookshop.ru/59350.html>.
6. Петров А.А. Компьютерная безопасность. Криптографические методы защиты [Электронный ресурс]/ Петров А.А.— Электрон. текстовые данные.— Саратов: Профобразование, 2019.— 446 с.— Режим доступа: <http://www.iprbookshop.ru/87998.html>.
7. Программно-аппаратные средства защиты информации [Электронный ресурс]: учебное пособие для студентов вузов по направлению подготовки «Информационная безопасность»/ Л.Х. Мифтахова [и др.].— Электрон. текстовые данные.— СПб.:

Интермедия, 2018.— 408 с.— Режим доступа: <http://www.iprbookshop.ru/73644.html>.

8. Рагозин Ю.Н. Инженерно-техническая защита информации [Электронный ресурс]: учебное пособие по физическим основам образования технических каналов утечки информации и по практикуму оценки их опасности — Электрон. текстовые данные.— СПб.: Интермедия, 2018.— 168 с.— Режим доступа: <http://www.iprbookshop.ru/73641.html>.

9. Скрипник Д.А. Общие вопросы технической защиты информации [Электронный ресурс] — Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 424 с.— Режим доступа: <http://www.iprbookshop.ru/52161.html>.

10. Соколов В.П., Тарасова Н.П. Кодирование в системах защиты информации [Электронный ресурс]: учебное пособие — Электрон. текстовые данные.— М.: Московский технический университет связи и информатики, 2016.— 94 с.— Режим доступа: <http://www.iprbookshop.ru/61485.html>.

11. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс] / Шаньгин В.Ф.— Электрон. текстовые данные.— Саратов: Профобразование, 2019.— 543 с.— Режим доступа: <http://www.iprbookshop.ru/87992.html>.

7.2. Дополнительная литература

1. Астахова А.В. Информационные системы в экономике и защита информации на предприятиях — участниках ВЭД [Электронный ресурс]: учебное пособие — Электрон. текстовые данные.— СПб.: Троицкий мост, 2014.— 216 с.— Режим доступа: <http://www.iprbookshop.ru/40860.html>.

2. Бурняшов Б.А. Меры защиты информации на уровне пользователя информационно-технологическими средствами [Электронный ресурс]: методические указания к самостоятельной работе студентов. Учебно-методическое пособие — Электрон. текстовые данные.— Саратов: Вузовское образование, 2014.— 55 с.— Режим доступа: <http://www.iprbookshop.ru/23077.html>.

3. Голиков А. М. Защита информации в инфокоммуникационных системах и сетях: учебное пособие [Электронный ресурс]. — Томск: ТУСУР, 2015. -Режим доступа: <https://edu.tusur.ru/publications/5262>

4. Голиков А. М. Защита информации от утечки по техническим каналам: учебное пособие. - Томск: Томский государственный университет систем управления и радиоэлектроники, 2015.

5. Петренко В.И., Мандрица И. В. Защита персональных данных в информационных системах. Курс лекций. — Ставрополь: СКФУ, 2013.

6. Сагдеев К. М., Петренко В.И., Чипига А. Ф. Физические основы защиты информации.— Ставрополь: Изд-во СКФУ, 2017.
7. Скрипник Д. А. Общие вопросы технической защиты информации [Электронный ресурс]. — М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— Режим доступа: <http://www.iprbookshop.ru/52161.html>.

7.3 Интернет-ресурсы

1. Безопасность информационных систем. URL: <http://intuit.valrkl.ru/course-1312/index.html>
2. Введение в информационную безопасность автоматизированных систем. URL: <http://baumanpress.ru/books/558/558.pdf>
3. Защита информации техническими средствами. URL: <https://books.ifmo.ru/file/pdf/975.pdf>
4. Защита информации. URL: <https://center-yf.ru/data/stat/zashchita-informacii.php>
5. Информационная безопасность и защита информации. URL: <https://www.sites.google.com/site/inftech11/home/sam/materialy-lekcii-informacionnaa-bezopasnost-i-zasita-informacii>
6. Информационные технологии. Основные термины и определения в области технической защиты информации. URL: https://ohranatruda.ru/ot_biblio/norma/392274/
7. Основные моменты технической защиты информации. URL: <https://camafon.ru/informatsionnaya-bezopasnost/tehnicheskaya-zashhita>

7.4. Перечень учебно-методических разработок

По дисциплине «Защита информации в технических системах» разработан практикум: Хакулов В. А., Карякин А. Т., Шаповалов В. А. “Организация проектной деятельности. Унифицированные проекты (модули)”- Нальчик, Каб.-Балк. ун.-т, 2018, 73 с. для студентов, позволяющие организовать работу по изучению дисциплины и создать условия для самостоятельной работы. Практикум издан в печатном и электронном вариантах и доступен для каждого студента. Методическое пособие содержит лабораторные работы по использованию унифицированных проектов (модулей), являющихся основой более сложных проектов.

7.5 Перечень профессиональных баз данных и информационно-справочных систем

1. ЭБД РГБ - Электронные версии полных текстов диссертаций и авторефератов из фонда Российской государственной библиотеки URL: <http://www.diss.rsl.ru>
2. SciverseScopus издательства «Эльзевир. Наука и технологии». Реферативная и аналитическая база данных URL: <http://www.scopus.com>

3. Электронная библиотека научных публикаций URL: <http://elibrary.ru>
4. Обзор СМИ России и зарубежья. Полные тексты + аналитика из 600 изданий по 53 отраслям URL: <http://polpred.com>
5. Федеральное агентство по техническому регулированию и метрологии URL: <https://www.gost.ru/portal/gost/home/standarts>

7.6 Программное обеспечение современных информационно-коммуникационных технологий

Windows 7, Microsoft Office (Word, Excel), Acrobat Reader, WinRaR, Delphi XE2 Professional № лицензии (License Certificate Number) 207406, Dev-C++ — свободная интегрированная среда разработки приложений для языков программирования C/C++. Открытая лицензия (GNU GPL), Python 3.6 IDE PyCharm Professional Edition является бесплатным для образовательных учреждений (свободное распространение), Arduino IDE Лицензия GNU General Public License, OpenCV | Лицензия BSD (Berkeley Software Distribution license), Ubuntu Лицензия GPL, Lazarus (Free Pascal).

8 Материально-техническое обеспечение дисциплины

По дисциплине «Защита информации в технических системах» имеются презентации по всем темам курса, позволяющие наиболее эффективно освоить представленный учебный материал. Имеются компьютерное и мультимедийное оборудование и программное обеспечение для выполнения лабораторных работ.

Тип аудитории, расположение	Оборудование и инвентарь аудитории	Программное обеспечение
Учебная аудитория для проведения занятий лекционного типа 02 ауд. (Условный номер №3; 360004, Кабардино-Балкарская Республика, г. Нальчик, ул. Чернышевского, д. 173)	1. Столы – 24 шт. 2. Стулья – 34 шт. 3. Персональные компьютеры 11 шт. 4. Сетевое оборудование для коммутации и доступа в Internet Cisco – 1 шт. 5. Переносные унифицированные модули на основе микроконтроллеров (12 шт.), других (12 шт.) электронных или электромеханических устройств автоматизации, визуализации результатов, мониторинга на основе цифровых, аналоговых датчиков и др., конкретная номенклатура модулей, устанавливаемых в аудитории, зависит от темы занятий. Обменный фонд стендов и унифицированных модулей хранится в ауд. 114 (Условный номер №2;	Windows 7. Microsoft Office 2013 (Word, Excel, Access, PowerPoint и пр.) Программы для работы с PDF (Acrobat Reader, Sumatra PDF, stduviewer) (свободное распространение) Архиваторы(7zip, WinRaR) (свободное распространение) Delphi XE2 Professional № лицензии (License Certificate Number) 207406 Dev-C++ свободная интегрированная среда разработки приложений для языков программирования C/C++. (свободное распространение) Python 3.6 IDE Py Charm Professional Edition является бесплатным для образовательных учреждений (свободное распространение) Среда для разработки ArduinoIDE (свободное распространение) Ubuntu Лицензия GPL (свободное распространение). Lazarus (FreePascal) RAD IDE(свободное распространение) КОМПАС-3D LT САПР для учебных целей, облегченная версия профессиональной системы КОМПАС-3D. (свободное распространение). InkScape векторный

	<p>360004, Кабардино-Балкарская Республика, г. Нальчик, ул. Чернышевского, д. 173) в металлическом шкафу, под замком и используются во время лекционных занятий.</p> <p>6. Проектор – 1 шт.</p> <p>7. Ноутбук – 1 шт.</p> <p>8. Экран. – 1 шт.</p> <p>9. Учебные стенды (из унифицированных модулей) для комплексной отладки и испытаний программно-аппаратных управляющих комплексов.</p>	<p>графический редактор (свободное распространение)</p> <p>3D-редактор Blender (свободное распространение)</p> <p>Simple-Scada 2 открытая версия с базовым функционалом, 64 тега (свободное распространение)</p> <p>Среда разработки для микроконтроллеров AVR Studio (свободное распространение)</p> <p>Coppelia Robotics V-REP PRO EDU V3.6.2 rev0 Non-limited EDUCATIONAL version. Free (свободное распространение)</p> <p>Среда для разработки Arduino IDE (свободное распространение)</p> <p>OpenCV (свободное распространение). Qt (свободное распространение)</p>
<p>Учебная аудитория для проведения занятий лекционного типа 103а ауд. (Условный номер №2; 360004, Кабардино-Балкарская Республика, г. Нальчик, ул. Чернышевского, д. 173)</p>	<p>1. Столы - 20 шт.</p> <p>2. Стулья – 21 шт.</p> <p>3. Персональные компьютеры - 10 шт.</p> <p>4. Сетевое оборудование для коммутации и доступа в Internet Cisco – 1 шт.</p> <p>5. Переносные унифицированные модули на основе микроконтроллеров (12 шт.), других (12 шт.) электронных или электромеханических устройств автоматизации, визуализации результатов, мониторинга на основе цифровых, аналоговых датчиков и др., конкретная номенклатура модулей, устанавливаемых в аудитории, зависит от темы занятий. Обменный фонд стендов и унифицированных модулей хранится в ауд. 114 (Условный номер №2; 360004, Кабардино-Балкарская Республика, г. Нальчик, ул. Чернышевского, д. 173) в металлическом шкафу, под замком и используются во время лекционных занятий.</p> <p>6. Проектор.</p> <p>7. Ноутбук.</p> <p>8. Интерактивная доска.</p> <p>9. Учебные стенды (из унифицированных модулей) для комплексной отладки и испытаний программно-аппаратных управляющих комплексов.</p>	<p>Windows 7. Microsoft Office 2013 (Word, Excel, Access, PowerPoint и пр.)</p> <p>Программы для работы с PDF (Acrobat Reader, Sumatra PDF, stduviewer) (свободное распространение)</p> <p>Архиваторы(7zip, WinRaR) (свободное распространение)</p> <p>Delphi XE2 Professional № лицензии (License Certificate Number) 207406</p> <p>Dev-C++ свободная интегрированная среда разработки приложений для языков программирования C/C++. (свободное распространение)</p> <p>Python 3.6 IDEPy Charm Professional Edition является бесплатным для образовательных учреждений (свободное распространение)</p> <p>Среда для разработки ArduinoIDE (свободное распространение)</p> <p>Ubuntu Лицензия GPL (свободное распространение).</p> <p>Lazarus (FreePascal) RAD IDE(свободное распространение)</p> <p>КОМПАС-3D LT САПР для учебных целей, облегченная версия профессиональной системы КОМПАС-3D. (свободное распространение).</p> <p>InkScape векторный графический редактор (свободное распространение)</p> <p>3D-редактор Blender (свободное распространение)</p> <p>Simple-Scada 2 открытая версия с базовым функционалом, 64 тега (свободное распространение)</p> <p>Среда разработки для микроконтроллеров AVR Studio (свободное распространение)</p> <p>Coppelia Robotics V-REP PRO EDU V3.6.2 rev0 Non-limited EDUCATIONAL version. Free (свободное распространение)</p> <p>Среда для разработки Arduino IDE (свободное распространение)</p> <p>OpenCV (свободное распространение). Qt (свободное распространение).</p>
<p>Учебная аудитория для проведения занятий семинарского типа 103а ауд. (Условный номер №2; 360004, Кабардино-Балкарская Республика,</p>	<p>1. Столы - 20 шт.</p> <p>2. Стулья – 21 шт.</p> <p>3. Персональные компьютеры - 10 шт.</p> <p>4. Сетевое оборудование для коммутации и доступа в Internet Cisco – 1 шт.</p> <p>5. Переносные унифицированные модули на основе микроконтроллеров (12 шт.), других (12 шт.) электронных или электромеханических устройств автоматизации, визуализации результатов, мониторинга на основе цифровых,</p>	<p>Windows 7. Microsoft Office 2013 (Word, Excel, Access, PowerPoint и пр.)</p> <p>Программы для работы с PDF (Acrobat Reader, Sumatra PDF, stduviewer) (свободное распространение)</p> <p>Архиваторы(7zip, WinRaR) (свободное распространение)</p> <p>Delphi XE2 Professional № лицензии (License Certificate Number) 207406</p> <p>Dev-C++ свободная интегрированная среда разработки приложений для языков программирования C/C++. (свободное распространение)</p> <p>Python 3.6 IDEPy Charm Professional Edition является бесплатным для образовательных учреждений (свободное распространение)</p> <p>Среда для разработки ArduinoIDE (свободное распростра-</p>

г. Нальчик, ул. Чернышевского, д. 173)	аналоговых датчиков и др., конкретная номенклатура модулей, устанавливаемых в аудитории, зависит от темы занятий. Обменный фонд стендов и унифицированных модулей хранится в ауд. 114 (Условный номер №2; 360004, Кабардино-Балкарская Республика, г. Нальчик, ул. Чернышевского, д. 173) в металлическом шкафу, под замком и используются во время лекционных занятий. 6. Проектор. 7. Ноутбук. 8. Интерактивная доска. 9. Учебные стенды (из унифицированных модулей) для комплексной отладки и испытаний программно-аппаратных управляющих комплексов.	нение) Ubuntu Лицензия GPL (свободное распространение). Lazarus (FreePascal) RAD IDE(свободное распространение) КОМПАС-3D LT САПР для учебных целей, облегченная версия профессиональной системы КОМПАС-3D. (свободное распространение). InkScape векторный графический редактор (свободное распространение) 3D-редактор Blender (свободное распространение) Simple-Scada 2 открытая версия с базовым функционалом, 64 тег (свободное распространение) Среда разработки для микроконтроллеров AVR Studio (свободное распространение) Coppelia Robotics V-REP PRO EDU V3.6.2 rev0 Non-limited EDUCATIONAL version. Free (свободное распространение) Среда для разработки Arduino IDE (свободное распространение) OpenCV (свободное распространение). Qt (свободное распространение)
--	---	--

9. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

Для студентов с ограниченными возможностями здоровья созданы специальные условия для получения образования. В целях доступности получения высшего образования по образовательным программам инвалидами и лицами с ограниченными возможностями здоровья университетом обеспечивается:

1. Альтернативная версия официального сайта в сети «Интернет» для слабовидящих.
2. Для инвалидов с нарушениями зрения (слабовидящие, слепые):
 - присутствие ассистента, оказывающего обучающемуся необходимую помощь, дублирование вслух справочной информации о расписании учебных занятий; наличие средств для усиления остаточного зрения, брайлевской компьютерной техники, видеоувеличителей, программ не визуального доступа к информации, программ-синтезаторов речи и других технических средств приема-передачи учебной информации в доступных формах для студентов с нарушениями зрения;
 - задания для выполнения на экзамене зачитываются ассистентом;
 - письменные задания выполняются на бумаге, надиктовываются ассистенту обучающимся.
3. Для инвалидов и лиц с ограниченными возможностями здоровья по слуху (слабослышащие, глухие):
 - на зачете/экзамене присутствует ассистент, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (он помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе записывая под диктовку);

- зачет/экзамен проводится в письменной форме.

4. Для инвалидов и лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, созданы материально-технические условия обеспечивающие возможность беспрепятственного доступа обучающихся в учебные помещения, объекты питания, туалетные и другие помещения университета, а также пребывания в указанных помещениях (наличие расширенных дверных проемов, поручней и других приспособлений):

- письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту;

- по желанию студента экзамен проводится в устной форме.

Обучающиеся из числа лиц с ограниченными возможностями здоровья обеспечены электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

Лист изменений (дополнений) в рабочей программе дисциплины (модуля) «Защита информации в технических системах» по направлению подготовки 27.03.04 «Управление в технических системах»

(специальности) (образовательная программа Информационные технологии в управлении техническими системами) на 2019 – 2020 учебный год

№ п/п	Элемент (пункт) РПД	Перечень вносимых изменений (дополнений)	Примечание

Обсуждена и рекомендована на заседании кафедры

наименование кафедры

протокол № _____ от «__» _____ 20__ г.

Заведующий кафедрой _____

подпись, расшифровка подписи, дата

Согласовано:*

Заведующий отделом комплектования

научной библиотеки _____

личная подпись расшифровка подписи дата

**Примечание: при внесении изменений в п. 4.7.1 РПД*