МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета _____ Бурковский А.В.

31 08 2018г.

РАБОЧАЯ ПРОГРАММА

Дисциплины

«Информационная безопасность и защита информации»

Направление подготовки 27.03.04 «Управление в технических системах»

Профиль "Управление и информатика в технических системах"

Квалификация выпускника бакалавр

Нормативный период обучения 4года

Форма обучения очная

Год начала подготовки 2018

Автор программы _____ Е.М. Васильев

Заведующий кафедрой
электропривода, автоматики
и управления в технических системах._____В.Л. Бурковский

Руководитель ОПОП_____ К.Ю. Гусев

Воронеж 2018

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1 Цель изучения дисциплины – формирование у студентов способности понимать сущность и значения информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны.

1.2 Задачи освоения дисциплины:

изучение доктрины информационной безопасности Российской Федерации, структуры государственной системы информационной безопасности;

ознакомление с законодательной базой по вопросам информационной безопасности и соответствующими нормативными документами;

владение криптографическими методами защиты информации;

приобретение навыков защиты информации криптографическими средствами.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Информационная безопасность и защита информации» относится к дисциплинам части, формируемой участниками образовательных отношений блока Б.1 учебного плана.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Информационная безопасность и защита информации» направлен на формирование следующих компетенций:

ОПК-9 - способность использовать навыки работы с компьютером, владеть методами информационных технологий, соблюдать основные требования информационной безопасности

ПК-6 - способность производить расчеты и проектирование отдельных блоков и устройств систем автоматизации и управления и выбирать стандартные средства автоматики, измерительной и вычислительной техники для проектирования систем автоматизации и управления в соответствии с техническим заданием.

Компетенция	**Результаты обучения, характеризующие сформированность компетенции**
ОПК-9	знать цели и задачи информационной безопасности, методы её обеспечения
	уметь применять полученные знания защиты информации в профессиональной деятельности.
	владеть способами и приёмами защиты информации криптографическими средствами
ПК-6	владеть приёмами расчёта криптографических средств защиты информации

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Информационная безопасность и защита информации» составляет 3 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры
		2
Аудиторные занятия (всего)	54	30
В том числе:		
Лекции	18	18
Лабораторные занятия	18	12
Практические занятия	18	
Самостоятельная работа	54	78
Курсовая работа	+	+
Виды промежуточной аттестации - зачет	+	+
Общая трудоемкость: академические часы зач.ед.	 108 3	 108 3

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Лаб. зан.	Практ	СРС	Всего, час
1	Введение	Основные понятия об информационной безопасности и защите информации. Доктрина информационной безопасности Российской Федерации. Структура государственной системы информационной безопасности. Структура законодательной базы по вопросам информационной безопасности. Способы защиты информации. Самостоятельное изучение. Государственные стандарты РФ в области защиты информации	2	-	2	10	14
2	Архитектура криптографических систем защиты информации	Основные понятия и определения криптографии Системы с открытым и закрытым ключом. Порядок их функционирования. До-	8	-	6	10	24

		стоинства и недостатки. Протоколы передачи данных в симметричных и несимметричных системах передачи данных Протоколы цифровой подписи и разделения ключа. Области применения этих протоколов. Самостоятельное изучение. Протоколы электронных платежей, голосования, обмена без передачи ключей.					
3	Криптографические алгоритмы	Шифры одноалфавитной и многоалфавитной замены. Анализ стойкости этих шифров. Абсолютно стойкий шифр замены. Шифры перестановок. Достоинства и недостатки этих шифров. Методы генерации случайных ключей. Способы проверки статистической независимости элементов ключа. Криптографические алгоритмы на основе односторонних функций.	8	18	10	34	70
		Итого	**18**	**18**	**18**	**54**	108

5.2 Перечень лабораторных работ

1. Шифры замены и криптоанализ зашифрованных сообщений
2. Программирование криптографических алгоритмов перестановок
3. Шифрование на основе однонаправленных функций
4. Генерирование криптографических ключей

5.3. Практические занятия .

1. Криптографические системы
2. Криптографические протоколы
3. Шифры замены
4. Многоалфавитные шифры замены
5. Шифры перестановок
6. Шифры на основе односторонних функций

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

Примеры тем курсовых работ

1. Разработка критерия криптографической стойкости шифров перестановок.
2. Анализ стойкости криптографического протокола голосования.
3. Разработка криптографического алгоритма порогового разделения секрета.
4. Анализ стойкости криптографического протокола цифровой подписи.
5. Разработка криптографического алгоритма многоалфавитной замены.
6. Разработка криптографического алгоритма маршрутной перестановки.
7. Исследование алгоритмов генерации случайных ключей.
8. Анализ криптографической системы без передачи ключей.
9. Разработка абсолютно стойкого шифра замены.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе:

«аттестован»;

«не аттестован».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Способ оценивания	Аттестован	Не аттестован
ОПК-9	знать цели и задачи информационной безопасности, методы её обеспечения	Работа на лекциях, ответы на теоретические вопросы	Активная работа на лекциях, ответы на теоретические вопросы	Неудовлетворительные ответы на теоретические вопросы
	уметь применять полу-	Решение стандарт-	Выполнение теста	Выполнение

	ченные знания защиты информации в профессиональной деятельности.	ных практических задач	на оценку "отлично", "хорошо" или "удвлетворительно".	теста на оценку "неудовлетворительно".
	владеть способами и приёмами защиты информации криптографическими средствами	Решение прикладных задач в конкретной предметной области,	Верное решение задач	Задачи не решены
ПК-6	владеть приёмами расчёта криптографических средств защиты информации	Решение прикладных задач в конкретной предметной области,	Верное решение задач	Задачи не решены

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются для очной формы обучения по следующей системе:

«зачтено»;
«не зачтено».

Компетенция	**Результаты обучения, характеризующие сформированность компетенции**	**Способ оценивания**	**Зачтено**	**Не зачтено**
ОПК-9	знать цели и задачи информационной безопасности, методы её обеспечения	Опрос	Полный ответ. Делаются обоснованные выводы. Демонстрируются глубокие знания. Демонстрируется умение анализировать материал.	Затрудняется ответить
	уметь применять полученные знания защиты информации в профессиональной деятельности.	Решение стандартных практических задач в форме теста	Выполнение теста на 70-100%	В тесте менее 70% правильных ответов
	владеть способами и приёмами защиты информации криптографическими средствами	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ПК-6	владеть приёмами расчёта криптографических средств защиты информации	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы. Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

7.2 Примерный перечень оценочных средств (типовые контрольные задания

или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

7.2.1 Примерный перечень вопросов для подготовки к тестированию

1. Основные понятия об информационной безопасности и защите информации. Доктрина информационной безопасности Российской Федерации.
2. Структура государственной системы информационной безопасности. Структура законодательной базы по вопросам информационной безопасности.
3. Способы защиты информации. Государственные стандарты РФ в области защиты информации.
4. Основные понятия и определения криптографии.
5. Системы с открытым и закрытым ключом. Порядок их функционирования. Достоинства и недостатки.
6. Протоколы передачи данных в симметричных и несимметричных системах передачи данных.
7. Протоколы цифровой подписи и разделения ключа. Области применения этих протоколов
8. Протоколы электронных платежей.
9. Протоколы голосования.
10. Протоколы обмена без передачи ключей.
11. Шифры одноалфавитной и многоалфавитной замены. Анализ стойкости этих шифров.
12. Абсолютно стойкий шифр замены.
13. Шифры перестановок. Достоинства и недостатки этих шифров.
14. Методы генерации случайных ключей. Способы проверки статистической независимости элементов ключа.
15. Криптографические алгоритмы на основе односторонних функций.

7.2.2 Примерный перечень заданий для решения стандартных задач

1.Что такое информационная безопасность:
а) действия по обеспечению информационной безопасности;
б) состояние защищённости в информационной сфере;
в) ограничение доступа к информации посторонним лицам;
г) скрытность хранения и передачи информации.

2. Что относится к защите информации?
а) действия по обеспечению информационной безопасности;
б) состояние защищённости;
в) ограничение доступа к информации посторонним лицам;
г) скрытность хранения и передачи информации.

3. Расположите способы защиты информации в порядке возрастания их стойкости:
а) скрытие факта передачи информации ;
б) ограничение доступа к носителю информации;
в) шифрование информации.
г) кодирование информации.

4. Что такое криптография?

а) способ кодирования сообщения;

б) способ шифрования сообщения;

в) способ передачи сообщения.

5. Что является количественной мерой стойкости шифра?

а) количество возможных вариантов ключа;

б) продолжительность времени, необходимого для перебора всех вариантов ключа ;

в) степень неизвестности принципа шифрования;

г) степень неизвестности протокола передачи информации

6. Что характерно для криптографической системы с закрытым ключом:

а) закрытый канал передачи информации;

б) закрытый канал для передачи ключа;

в) закрытый способ шифрования;

г) закрытый ключ.

7. Что характерно для криптографической системы с открытым ключом:

а) открытый канал передачи информации;

б) открытый канал для передачи ключа;

в) открытый способ шифрования;

г) открытый ключ.

8. Какую систему передачи информации использует протокол цифровой подписи:

а) систему с открытым ключом;

б) систему с закрытым ключом;

в) система с разделением секрета;

г) система анонимной передачи данных.

9. Количество вариантов ключа длиной 5 в шифре многоалфавитной замены для сообщения, содержащего 10 символов:

а) 5^{10};

б) 10^{5};

в) 5*10;

г) (10-5)!

10. Количество вариантов ключа в шифре замены для алфавита мощностью 10 символов:

а) 10;

б) 10!;

в) 9;

г) (10-1)!

11. Какие матрицы может быть использованы в качестве ключа для шифра перестановки:

11.1

1	0	0	0
0	0	1	0
0	0	0	1
0	1	0	0

11.2

1	0	0	0
0	0	1	0
0	0	0	1
1	0	0	0

11.3

1	0	0	0
0	1	0	0
0	0	1	0
0	0	0	1

11.4

1	0	0	1
1	1	0	0
0	1	1	0
0	0	1	1

7.2.3 Примерный перечень заданий для решения прикладных задач

По заданному шифротексту вскрыть ключ шифра замены и дешифровать текст.

Вариант 1.

4[4?@]%wft]f\7[q@f@7@q[q@i5%f5tq[%[i[7[4%q@q[№_[_[*6@*4@w@q[4q[4[@6%7:@[f
qt6%4*15;8\@i[rt5itqq\@*17\%№_[_[[?_t47@q[s79q*6s\i[_[8*№_[%?;st@3@qt@w6t_:%ws
@?:=[7*it_:?9ti[?_[9qq[[?_t4t7%?:_@i@5:4ft0s@_[7:=[?_t5%=%%?_t5*]%[q%?8[_5@7%wt[
1[5[s[8%s[8[8][s%7%wt?=[_%q[04[w%7%?:?5@f9_%r=t8%?[]5tq994[4?@86%7[0s*]%[f@5
@1t9s@5@4q;[_%w7%rq@1[wti*?_@q%9

Вариант 2.

i[4@№@5t8[q%?][s%7%?:48@?_@q@15[8=[5tw1[4t5%4t7%%4?@[f[sq[8[_[8№_[f*s@_№t?
_[%_96@7[4ws\]t7%[it?7%4[i[179s\4t94?_[5[q*i5t4[1[f@5@1twtf%5;?*1s@?_5[%7?9f[7:r[0q
[4\0i[?@7[=?7*]%[__*sts[][s%7%5twq\@_[_i@54\08*6%==[_[5\0_5%?_t?7%rq%87e_qtwtsqt
s*8t7i[?@7%_:?9qt[?_5[4@f\7№@7[4@=w[5=%0%4\1ts7%4\04@5q[5t??*s%4r%0№_[7*№r
@d_[0w@87%@8*q@?\?=t_:[?_5[45t?_9q*7?9qti9_:?7%rq%84@5?_%q

Вариант 3.

@*w@q:=[07@q_[0t*_;1[8f\7[1s@5tw8@?_%_:?9%itrq@%7@?*%f[7[_+*?791*r=[0t?q%6q
@0?_[5[q\wt8@7=[0=5%4[0i5[_[=[0=ft0sef7%w=[i[s№t7%4t7s5*1[0[?_5[4=[_[5\0qtw\4t7%_[
i[s8[1[0_[i[sq[1[0i[s8[1ti[q9_q[№@1[qe]4t_t7[qt?4[@0w@87@f5t7%ws@?:ti[№@8*i[sq[1tq
%[sqts*rtf\q@[f29?q%7tt_@i@5:q@[f29?q%_%i[st4q[4\4t7%7?i[_=q*4r%0?9№@0_[9w\=%i[
r7[t9w\=*%w4@?_q[№@8№*sq@0_@88%7@0s@5@4q9qt?4[@84@=*i[4%st7t4?9=[@8%8
[q@@i[sq%8t7%?:4s5@4q[?_%44@5]i[f%5;?@f[5[st_\@=twt=%?_t4%_:%5=*_?=%0[?_5[1i[

Вариант 4.

s4[5t№%4t7%=q@0qtq[№@4=*_[51[4\@7;s%?q*;3%@4_*%s5*1*;?_[5[q\4@w7%i[4[s@t5
@?_tq_[4%wt4%s@4i598[i[q[?*[f6%_[0f@5@1_[6@i[s15@ft7%=q@8*5tw6%1t7%=[?_5\4t5
%7%*]*%w4\7[47@qq[0_*_6@5\f\s4ti[7q\]sq915[][_t7ws@?:f[08@6s*=[7№t=[4+t8%wtq94r
%8%[?_5[4%it5_%wtqt8%=[_[5\@r7%47[s=t]qti5%?_*i?[f[%]f@5@1[4[_=[7№t=[4+@4[?_t7
?94ft0s@?5*f7@qq\0%8%qt4@5]q@8=5t;*1[7[8\?=%ft5t=4=[_[5[84i[?7@sq%@1[s\i[=5t?q\8
7@_t8=[1st_@i7[6%7=t=_t5t=tqf[1[s*7

Вариант 5.
f<drk9z9v9zdhf71k7j>149]ktrjqj78>b94>0s6]75>dt5>9jr08749wdttr57twf]=n7wq929jrk9zk>59]nh67rd987]7zt6jts<69]9d9j>=j17]wtj\r0k>67d0k>j9w9rj>z89rj>d7q9]k75r9f9]94<k>87b891>1f<]>87rjk76d>qhjr59]1>0d9j0j5kt41>6dtz>rkhjk>rk9zh7jq9z7w>d767w>dhrk9zrj>k75tjr049]ktrj<w67rd98kt9n]hrj0vt97rj>j1td\8>k>87]7z9tnk>4<5>=jq9]961>wttj7d980k79d7b96717j7]7whf9b>d67j71j7b9]>4w<d7t7k7]>4w01d76785787[k>ij7wb9dj7wd7b94>0s69]9f9z>0k>jhrj7]7khk7q\=7rj>5tdrd98<

Вариант 6.
59rk>578<r7ft]>9j]78rj59kk<945h1tf<5>9j87dz7k9w7b92\67k0j\qj7ij7578>fhd\1>9jtdtj9j9]95>f7]w7qhjtdtd0zh21th]q>j5r95w9rj9rdt5>9jr0578kh69rk=578<tk>8k9[r7zd>rk75r9whfd99jf91>r5r7zd>rttr5787[5>d\82k96n]t6tjtj>tkrj59kk7hn>9j5<6\5r9ij7rj]>kk7969k\96jts5<2d7t469rkt59r9kk9[578<9v9k9r17d\178k9[1>1>0ktfh8\k989d0t59r\ij7jk959]70jk<[nd>w5d9rh6]t]78>k>qk9j4>1]<5>j\s59j>wtj]>5>wt49d9k9=vtwtwn>wtj7k17[w7d787[67]7rd\=j]7z>j9d\k7rw7j]9j\1>16]t]78>4>f7jdt57hft]>9j85>]>4>5z78r57[b9dj<[rhn7[tw9]j5<[17rj0178tk]>459rk7[7k>4>1]<5>

Вариант 7.
9j9z77jk>29z7zd>4>s59j>wt8]hz7[]>47r9k\=rk9z7w9v9s59jhj7]9ntt7d\n>ttn47d7j<9r9]9b1t9v9tr9[q>r8<w0jr07j6]t17rk759kt06jtq91k7k95ktnj969]\89d77ktbt5hjk7tn5]9w06]72d7r9[q>rh8t5d0=jtz7r678rj5h=jwk7b9rj57wr57twt1]>r7j7[rtkt9s59jkt1t459487q17[t4]981>676>8>9jr0k7j7b9h8t5d09j57dq\9d<17d98]>rj>0dk>d9rk7[87]7z97rj>dr0k>574tk>ij7jk>5741>1fh8j7qh09z7k>d9j9d7t49d75<ntr7rk75<n2t291wk7b9rj57r9w0kr7qh5rj5h0675>d9kk7[f9]94907j8<n>dk>k9[trw7j]9dk>f7d\2h=q9]9whnhj74>f<5>099j7760j\rt4hwd9kt9w1k9[5745]>v>0r\wk91>4>d7r\fh8j7q9]

Вариант 8.
9whn>jhjb9k>zd>4>n7895>d>r\5r57t6]74]>qk<9r89d>kk<91>1fh8j7t449d9k7z72hw>789b8<8>r]98tr9]<n9v9k9789j<n89]95\95tq>rj<n1hrj757k>f<d>49d9k>0t5j7b95]9w0q9]94ijh49d9k\05t89dr4>8tk99q>rj<9f9d<9f9]941tk717z8>0678k0dr0t4>n7j9d6]7rjtj\r0r49d9k7[q9]9whn7[wk9671>4>d7r\fh8j7r4>8tk99tk9f<d75t8k7f9]9471qj7b9ij7j>179tdtij70r>w5<8hw>dfh8j7f<dtf9]941ttdttdtq9]9whn>789d>r\5j75]9w01>107j8<n>d8k9wk>k9f9f<dtk>78k7[5<r7j9172>q\tn57rj<k>8]hz7[6d<d7z]7wk<[k9trqtrdtw<[3d7j1hq95<n7fd>175w<k9w7zdth4k>j\qj7k>rjh6>9jtqj76]7n78tjst1d7ktdt>kjtst1d7k57jj969]\59q9]7w5r9tr1>4>d7r\tw9kk75ij7j59q9]r759]2tdr087dz7b8>kk<[69]957]7j69]9n787jk9789j7[59rk<149d9k9=v9[59rk9

7.2.4 Примерный перечень вопросов для подготовки к зачету

1. Основные понятия об информационной безопасности и защите информации. Доктрина информационной безопасности Российской Федерации.
2. Структура государственной системы информационной безопасности. Структура законодательной базы по вопросам информационной безопасности.
3. Способы защиты информации. Государственные стандарты РФ в области защиты информации.

4. Основные понятия и определения криптографии.
5. Системы с открытым и закрытым ключом. Порядок их функционирования. Достоинства и недостатки.
6. Протоколы передачи данных в симметричных и несимметричных системах передачи данных.
7. Протоколы цифровой подписи и разделения ключа. Области применения этих протоколов
8. Протоколы электронных платежей.
9. Протоколы голосования.
10. Протоколы обмена без передачи ключей.
11. Шифры одноалфавитной и многоалфавитной замены. Анализ стойкости этих шифров.
12. Абсолютно стойкий шифр замены.
13. Шифры перестановок. Достоинства и недостатки этих шифров.
14. Методы генерации случайных ключей. Способы проверки статистической независимости элементов ключа.
15. Криптографические алгоритмы на основе односторонних функций.

7.2.5 Примерный перечень вопросов для подготовки к экзамену

Не предусмотрено учебным планом

7.2.6. Методика выставления оценки при проведении текущего контроля

Зачёт с оценкой проводится по тест-билетам, каждый из которых содержит два вопроса и задачу в форме теста.

За ответы на вопросы билета выставляется:

5 баллов, если ответы на поставленные вопросы в билете излагаются логично, последовательно и не требуют дополнительных пояснений. Делаются обоснованные выводы. Демонстрируются глубокие знания базовых положений курса;

4 балла, если ответы на поставленные вопросы излагаются систематизировано и последовательно. Материал излагается уверенно. Демонстрируется умение анализировать материал, однако не все выводы носят аргументированный и доказательный характер;

3 балла, если имеются нарушения в последовательности изложения. Демонстрируются поверхностные знания вопроса. Имеются затруднения с выводами;

2 балла, если материал излагается непоследовательно, сбивчиво, не представляет определенной системы знаний;

0 баллов, если обучающийся затрудняется ответить на вопрос.

За выполнение теста на 90-100% выставляется 5 баллов, на 80—90% - 4 балла, на 70-80% - 3 балла, 50-60% - 2 балла; 40-50 % - 1 балл; менее 40 % - 0 баллов.

Максимальное количество набранных баллов – 15.

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 7 баллов.

2. Оценка «Удовлетворительно» ставится в случае, если студент набрал от 7 до 9 баллов

3. Оценка «Хорошо» ставится в случае, если студент набрал от 10 до 12 баллов.

4. Оценка «Отлично» ставится, если студент набрал от 13 до 15 баллов.

Студент аттестуется, при получении оценки «Удовлетворительно» или «Хорошо»

или «Отлично». При получении оценки «Неудовлетворительно» студент не аттестуется.

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Введение	ОПК-9, ПК-6	Тесты, проверочные задания
2	Архитектура криптографических систем защиты информации	ОПК-9, ПК-6	Тесты, проверочные задания
3	Криптографические алгоритмы	ОПК-92, ПК-6	Тесты, проверочные задания

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

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методики выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

1. Радько Н.М. Защита информации в беспроводных сетях [Электронный ресурс] : Учеб. пособие. - Электрон. текстовые, граф. дан. (835 072 байт). - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2010

2. Кольцов А.С. Информационная безопасность и защита информации [Электронный ресурс] : Учеб. пособие. - Электрон. текстовые, граф. дан. (4,5 Мб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2013.

3. Матвеев Б.В Защита информации в телекоммукационных системах : учеб. пособие. - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2007. - 282 с.

4. Радько Н.М. Защита информации в беспроводных сетях [Электронный ресурс] : Учеб. пособие. - Электрон. текстовые, граф. дан. (835 072 байт). - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2010

5. Чопоров О.Н. Защита информации и информационная безопасность [Электронный ресурс] : Учеб. пособие. - Электрон. текстовые, граф. дан. (1,8 Мб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2012.

6. Матвеев Б.В Защита информации в каналах связи : Лабораторный практикум: Учеб. пособие. - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2008. - 249 с.

7. Паринов А.В. Информационная безопасность и защита информации [Электронный ресурс] : Учеб. пособие. - Электрон. дан. (1 файл : 811 Кб). - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2007.

8. Паринов А.В. Информационная безопасность и защита информации : Учеб. пособие. - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2009. - 113 с.

9. Алексеев В.А. Методы и средства криптографической защиты информации [Электронный ресурс]: методические указания к проведению лабораторных работ по курсу «Методы и средства защиты компьютерной информации»/ Алексеев В.А.— Электрон. текстовые данные.— Липецк: Липецкий государственный технический университет, ЭБС АСВ, 2009.— 16 с.— Режим доступа: http://www.iprbookshop.ru/17710.html.— ЭБС «IPRbooks»

10. Качановский Ю.П. Основные технические, программные и организационные меры защиты информации при работе с компьютерными системами [Электронный ресурс]: методические указания к проведению лабораторной работы по курсу «Информатика»/ Качановский Ю.П., Широков А.С.— Электрон. текстовые данные.— Липецк: Липецкий государственный технический университет, ЭБС АСВ, 2014.— 24 с.— Режим доступа: http://www.iprbookshop.ru/55120.html.— ЭБС «IPRbooks»

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

Лицензионное программное обеспечение
MicrosoftOfficeWord 2013/2007
MicrosoftOfficeExcel 2013/2007
MicrosoftOfficePowerPoint 2013/2007
MatLab
Windows Professional 8.1 (7 и 8) Single Upgrade MVL A Each Academic

Свободное ПО
OpenOffice
Mozilla Firefox
Zip

Ресурсы информационно-телекоммуникационной сети «Интернет»
http://www.edu.ru/
Образовательный портал ВГТУ
https://electrono.ru

https://www.tehnari.ru/
https://ieeexplore.ieee.org/Xplore/home.jsp
https://www.sql.ru/

Информационные справочные системы
http://window.edu.ru
https://wiki.cchgeu.ru/

Современные профессиональные базы данных
База данных zbMath
Адрес ресурса: https://lib.tusur.ru/ru/resursy/bazy-dannyh/zbmath
Association for Computing Machinery, ACM
Адрес ресурса: https://dl.acm.org/contents_dl.cfm
Единый портал инноваций и уникальных изобретений
Адрес ресурса: http://innovationportal.ru/
Инновации в России
Адрес ресурса: http://innovation.gov.ru/
Росстандарт. Федеральное агентство по техническому регулированию и метрологии
Адрес ресурса: https://www.gost.ru/portal/gost/

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Дисплейный класс, оснащенный компьютерами с доступом в Интернет и программным обеспечением, необходимым для выполнения заданий и лабораторных работ

10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «Информационная безопасность и защита информации» читаются лекции, проводятся лабораторные занятия.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Лабораторные занятия направлены на приобретение практических навыков логического синтеза.

Контроль усвоения материала дисциплины производится проверкой заданий.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей,

	справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Лабораторные занятие	Выполнение лабораторных работ, содержащих прикладные задания по моделированию и анализу цифровых систем.
Практические занятия	Практические занятия способствуют овладению практических приёмов решения задач и выполнения курсовой работы
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточной аттестации.
Подготовка к промежуточной аттестации	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед зачетом с оценкой три дня эффективнее всего использовать для повторения и систематизации материала.

Лист регистрации изменений

№ п/п	Перечень вносимых изменений	Дата внесения изменений	Подпись заведующего кафедрой, ответственной за реализацию ОПОП
1	Актуализирован раздел 8.2 в части состава используемого лицензионного программного обеспечения, современных профессиональных баз данных и справочных информационных систем	31.08.2019	
2	Актуализирован раздел 8.2 в части состава используемого лицензионного программного обеспечения, современных профессиональных баз данных и справочных информационных систем	31.08.2020