Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Дагестанский государственный технический университет»

РЕКОМЕНДОВАНО К УТВЕРЖДЕНИЮ
Директор филиала ДГТУ в г.Дербенте И.М. Мейланов,
________________________.
Подпись ИОФ

20-08. 2018г.

УТВЕРЖДАЮ

Проректор по учебной работе
________ **Н.С.Суракатов**
Подпись ИОФ

24. 09. 2018г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина: Б1.Б.18 Информационная безопасность
наименование дисциплины по ООП и код по ФГОС

для направления 09.03.03- «Прикладная информатика»
шифр и полное наименование направления

по профилю 09.03.03- «Прикладная информатика в экономике»
шифр и полное наименование профиля

Факультет: филиал ДГТУ в г. Дербенте
наименование факультета , где ведется дисциплина

Кафедра Естественнонаучных, гуманитарных, общепрофессиональных и специальных дисциплин
наименование кафедры, за которой закреплена дисциплина

Квалификация выпускника (степень) бакалавр
бакалавр

Форма обучения очная, курс 3-4 семестр(ы) 6-7
очная, заочная, др.

Всего трудоемкость в зачетных единицах (часах) 7 ЗЕТ (252 час.)

лекции 34 (час) экзамен . 7 сем. 1 ЗЕТ (36 час.)
(семестр)

практические (семинарские) занятия - (час); зачет 6
(семестр)

лабораторные занятия 68 (час); самостоятельная работа 114 (час);

курсовой проект (работа, РГР) - (семестр).

Зав. кафедрой ЕГО и СД ________________ Г.М. Гусейнова
подпись

Начальник УО ________________ Э.В. Магомаева
подпись

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций примерной ООП ВО по направлению 09.03.03- «Прикладная информатика» по профилю «Прикладная информатика в экономике».

Программа одобрена на заседании выпускающей кафедры от 06.09.2018 года, протокол № 1.

Зав. выпускающей кафедрой по данному профилю

_______________ Г.М. Гусейнова
подпись И.О.Ф

ОДОБРЕНО
Методическим советом филиала
09.00.00
шифр и полное наименование

Прикладная информатика
направления

Председатель к.ф.н., Г.М.Гусейнова
____
подпись, ИОФ

12.09 201 8 г.

АВТОР ПРОГРАММЫ
_______________ Джумалиева Е.Р.
подпись, И.О.Ф

ст.преподаватель
ФИО, уч.степень, ученое звание, подпись

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ.

Цель изучения дисциплины: обучение студентов основам защиты информации в информационных системах и формирование у них навыков использования существующих пакетов программ и технических средств по информационной безопасности в их дальнейшей деятельности.

Задачи изучения дисциплины: приобретение студентами прочных знаний и практических навыков в области, определяемой целью курса.

2. Место дисциплины в структуре ООП ВО

Дисциплина входит в базовую часть УП (Б1.Б.18)

3. Требования к уровню освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:
общекультурных:ОК4, ОПК1,4, ПК6,11, 13,15,18,21
способностью использовать основы правовых знаний в различных сферах деятельности (ОК-4);
Общепрофессиональных:
– способность использовать нормативно-правовые документы, международные и отечественные стандарты в области информационных систем и технологий (ОПК-1);
способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением ин формационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-4);
Профессиональных:
способностью собирать детальную информацию для формализации требований пользователей заказчика (ПК-6);
способностью эксплуатировать и сопровождать информационные системы и сервисы (ПК-11);
способностью осуществлять инсталляцию и настройку параметров программного обеспечения информационных систем (ПК-13);
способностью осуществлять тестирование компонентов информационных систем по заданным сценариям (ПК-15);
способностью принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью (ПК-18);
способностью проводить оценку экономических затрат и рисков при создании информационных систем (ПК-21);
В результате изучения дисциплины студенты должны:
Знать: цели, задачи, принципы и основные направления обеспечения информационной безопасности личности, общества, государства; основные термины по проблематике информационной безопасности; правовые аспекты обеспечения информационной безопасности; методологию создания систем защиты информации; перспективные направления развития систем и методов защиты информации; угрозы информационной безопасности; современные подходы к построению систем защиты информации; компьютерную систему, как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности;
Уметь: выявлять и классифицировать угрозы информационной безопасности, разрабатывать модели злоумышленников, разрабатывать политики информационной безопасности организации, реализовывать защиту информационных систем от компьютерных вирусов и других вредоносных программ; применять методы и средства защиты конфиденциальной информации, включая криптографические средства.
Владеть: навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем; правилами и приемами защиты сведений, составляющих государственную тайну, коммерческую тайну, а также персональных данных.

4. Структура и содержание дисциплины(модуля)

Общая трудоемкость дисциплины составляет 7ЗЕТ– 252час, в том числе – лекционные 34 часов, лабораторная работа 68 часов, СРС 114 часов, форма отчетности:6 семестр – зачет 7 семестр экзамен

4.1.Содержание дисциплины.

№ п/п	Раздел дисциплины тема лекции и вопросы	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Формы текущего * контроля успеваемости (по срокам текущих аттестаций в семестре) Форма промежуточной аттестации (по семестрам)
				ЛК	ПЗ	ЛР	СР	
Семестр 6								
1	ЛЕКЦИЯ 1. Проблема обеспечения ИБ. Основные понятия 1.Основные понятия ИБ. 2.Информация, защищаемая информация, ценность информации, уровень секретности. 3.Объекты защиты информации. 4.Угрозы безопасности информации, основные понятия: безопасность, конфиденциальность, целостность, доступность, утечка информации; несанкционированный доступ к информации.	**1**	1-3	4		7	11	Входной контроль
2	ЛЕКЦИЯ 2. Угрозы ИБ 1.Классификация угроз безопасности: каналы утечки, воздействия. 2.Прямые и косвенные каналы утечки данных.	**1**	5-7	3		6	13	Аттестационная работа №1
3	ЛЕКЦИЯ 3. Основы теории ИБ 1.Модель потенциального нарушителя. 2.Способы мошенничества в информационных системах. 3.Основные способы реализации угроз ИБ. 4.Основные понятия теории ИБ.	**1**	9-11	3		7	13	Аттестационная работа №2
4	Лекция 4. Оценка эффективности систем защиты информации 1.Принципы организации систем обеспечения безопасности данных. 2.Требования, предъявляемые к системам обеспечения безопасности данных. 3. Понятие мониторов безопасности. 4.Физические средства защиты информации	**1**	13-15	3		7	11	Аттестационная работа №3
5	ЛЕКЦИЯ 5. Нормативные руководящие документы в сфере обеспечения ИБ 1 Понятие политики безопасности. Дискреционные политики безопасности. Мандатные политики	**1**	17	4		7	11	

	безопасности 2 Модель безопасности информационных потоков. 3 Показатели эффективности систем защиты информации. Способы оценки эффективности систем защиты информации. 3 Руководящие документы Гостехкомиссии в сфере обеспечения ИБ							
Семестр 7								
6	ЛЕКЦИЯ 6. Программно-технические средства обеспечения ИБ 1.Основные понятия теории ИБ. 2.Принципы организации систем обеспечения безопасности данных. 3.Требования, предъявляемые к системам обеспечения безопасности данных. 4.Понятие мониторов безопасности. 5.Физические средства защиты информации	**1**	1-3	4		7	11	Входной контроль
7	ЛЕКЦИЯ 7. Межсетевые экраны 1.Руководящие документы Гостехкомиссии в сфере обеспечения ИБ. «Общие критерии». 2.Структура. Основные понятия. 3.Программно-технические средства обеспечения ИБ. 4.Межсетевые экраны.	**1**	5-7	3		7	13	Аттестационная работа №1
8	ЛЕКЦИЯ 8. Борьба с компьютерными вирусами 1.Типы компьютерных вирусов. 2.Методы борьбы с компьютерными вирусами.	**1**	9-11	3		7	13	Аттестационная работа №2
9	ЛЕКЦИЯ 9. Криптографические методы 1.Федеральный стандарт США на шифрование данных (стандарт DES). 2.Отечественный стандарт шифрование данных. 3. Шифрование с открытым ключом, алгоритм RSA.	**2**	13-15	3		7	11	Аттестационная работа №3
10	ЛЕКЦИЯ 10. Построение защищённых виртуальных сетей 1.Понятие, назначение и основные функции защищённой виртуальной сети. 2.Средства построения защищённой виртуальной сети. 3.Туннелирование в протоколах различных уровней.	**2**	17	4		6	11	Посещение занятий, тесты.
	Итого		**17**	**34**		**68**	**114**	**Экзамен 1 ЗЕТ 36 час**

4.2 Содержание лабораторных занятий

№ п/п	№ лекции из рабочей программы	Наименование лабораторного (практического, семинарского) занятия	Количество часов	Рекомендуемая литература и методические разработки (№ источника из списка литературы)
1	2	3	4	5
1	Лк.1	1 Основные понятия ИБ. 2 Угрозы безопасности информации, основные понятия: безопасность, конфиденциальность, целостность, доступность, утечка информации; несанкционированный доступ к информации.	6	1,2, 3
2	Лк.2	1 Классификация угроз безопасности. 2 Прямые и косвенные каналы утечки данных.	8	1,8
3	Лк.3	1 Модель потенциального нарушителя. 2 Способы мошенничества в информационных системах.	6	1,5, 6, 8, 9, 11
4	Лк.4	1 Принципы организации систем обеспечения безопасности данных. 2 Требования, предъявляемые к системам обеспечения безопасности данных.	8	1,7
5	Лк.5	1 Понятие политики безопасности. 2 Гостехкомиссии в сфере обеспечения ИБ.	6	1,7
6	Лк.6	1 Принципы организации систем обеспечения безопасности данных. 2 Понятие мониторов безопасности.	8	1,2, 3
7	Лк.7	1 Руководящие документы Гостехкомиссии в сфере обеспечения ИБ. 2 Межсетевые экраны.	6	1,8
8	Лк.8	1 Типы компьютерных вирусов. 2 Методы борьбы с компьютерными вирусами.	6	1,5, 6, 8, 9, 11
9	Лк.9	1 Федеральный стандарт США на шифрование данных (стандарт DES). 2 Шифрование с открытым ключом, алгоритм RSA.	8	1,7
10	Лк.10	1 Средства построения защищённой виртуальной сети. 2 Туннелирование в протоколах различных уровней.	6	1,2, 3
		ИТОГО	**68**	

4.3 Тематика для самостоятельной работы студентов

№	Тематика по содержанию дисциплины,	Количество	Рекомендуемая	Формы

п/п	выделенная для самостоятельного изучения	часов из содержания дисциплины	литература и источники информации	контроля СРС
1	2	3	4	5
1	1 Основные понятия ИБ. 2 Угрозы безопасности информации, основные понятия: безопасность, конфиденциальность, целостность, доступность, утечка информации; несанкционированный доступ к информации.	11	1,2,3,4	Отчет
2	1 Классификация угроз безопасности. 2 Прямые и косвенные каналы утечки данных.	13	Интернет, 10	Отчет
3	1 Модель потенциального нарушителя. 2 Способы мошенничества в информационных системах.	13	4,7,8	Отчет
4	1 Принципы организации систем обеспечения безопасности данных. 2 Требования, предъявляемые к системам обеспечения безопасности данных.	11	4,15	Отчет
5	1 Понятие политики безопасности. 2 Гостехкомиссии в сфере обеспечения ИБ.	11	1,2,11,12	Отчет
6	1 Принципы организации систем обеспечения безопасности данных. 2 Понятие мониторов безопасности.	11	Интернет , 1	Отчет
7	1 Руководящие документы Гостехкомиссии в сфере обеспечения ИБ. 2 Межсетевые экраны.	11	1, интернет	Отчет
8	1 Типы компьютерных вирусов. 2 Методы борьбы с компьютерными вирусами.	11	1, интернет	Отчет
9	1 Федеральный стандарт США на шифрование данных (стандарт DES). 2 Шифрование с открытым ключом, алгоритм RSA.	11	13, 4, 5	Отчет
10	1 Средства построения защищённой виртуальной сети. 2 Туннелирование в протоколах различных уровней.	11	14, 15, 5, 6	Отчет
	ИТОГО	**114**		

. Структура и содержание дисциплины(модуля) по заочной форме обучения

Общая трудоемкость дисциплины составляет 7ЗЕТ– 252час, в том числе – лекционные 8 часов, лабораторная работа 18 часов, СРС 213 часов, форма отчетности:4,5 курс – зачет /экзамен

4.4.Содержание дисциплины.

№ п/п	Раздел дисциплины тема лекции и вопросы	курс	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Формы текущего * контроля успеваемости (по срокам текущих аттестаций в семестре) Форма промежуточной аттестации (по семестрам)
				ЛК	ПЗ	ЛР	СР	

курс 4								
1	ЛЕКЦИЯ 1. Проблема обеспечения ИБ. Основные понятия 1.Основные понятия ИБ. 2.Информация, защищаемая информация, ценность информации, уровень секретности. 3.Объекты защиты информации. 4.Угрозы безопасности информации, основные понятия: безопасность, конфиденциальность, целостность, доступность, утечка информации; несанкционированный доступ к информации.	**4**		2		2	11	
2	ЛЕКЦИЯ 2. Угрозы ИБ 1.Классификация угроз безопасности: каналы утечки, воздействия. 2.Прямые и косвенные каналы утечки данных.	**4**		2		2	11	
3	ЛЕКЦИЯ 3. Основы теории ИБ 1.Модель потенциального нарушителя. 2.Способы мошенничества в информационных системах. 3.Основные способы реализации угроз ИБ. 4.Основные понятия теории ИБ.	**4**				2	11	
4	Лекция 4. Оценка эффективности систем защиты информации 1.Принципы организации систем обеспечения безопасности данных. 2.Требования, предъявляемые к системам обеспечения безопасности данных. 3. Понятие мониторов безопасности. 4.Физические средства защиты информации	**4**				2	11	
5	ЛЕКЦИЯ 5. Нормативные руководящие документы в сфере обеспечения ИБ 1 Понятие политики безопасности. Дискреционные политики безопасности. Мандатные политики безопасности 2 Модель безопасности информационных потоков. 3 Показатели эффективности систем защиты информации. Способы оценки эффективности систем защиты информации. 3 Руководящие документы Гостехкомиссии в сфере обеспечения ИБ	**4**				1	11	
				4		9	55	зачет
Курс 5								
6	ЛЕКЦИЯ 6. Программно-технические средства обеспечения ИБ	**5**		2		2	31	

	1.Основные понятия теории ИБ. 2.Принципы организации систем обеспечения безопасности данных. 3.Требования, предъявляемые к системам обеспечения безопасности данных. 4.Понятие мониторов безопасности. 5.Физические средства защиты информации							
7	ЛЕКЦИЯ 7. Межсетевые экраны 1.Руководящие документы Гостехкомиссии в сфере обеспечения ИБ. «Общие критерии». 2.Структура. Основные понятия. 3.Программно-технические средства обеспечения ИБ. 4.Межсетевые экраны.	**5**		2		2	31	
8	ЛЕКЦИЯ 8. Борьба с компьютерными вирусами 1.Типы компьютерных вирусов. 2.Методы борьбы с компьютерными вирусами.	**5**				2	31	
9	ЛЕКЦИЯ 9. Криптографические методы 1.Федеральный стандарт США на шифрование данных (стандарт DES). 2.Отечественный стандарт шифрование данных. 3. Шифрование с открытым ключом, алгоритм RSA.	**5**				2	31	
10	ЛЕКЦИЯ 10. Построение защищённых виртуальных сетей 1.Понятие, назначение и основные функции защищённой виртуальной сети. 2.Средства построения защищённой виртуальной сети. 3.Туннелирование в протоколах различных уровней.	**5**				1	34	
	Итого	**5**		**4**		**9**	**158**	**Экзамен**
				8		**18**	**213**	

4.5 Содержание лабораторных занятий

№ п/п	№ лекции из рабочей программы	Наименование лабораторного (практического, семинарского) занятия	Количество часов	Рекомендуемая литература и методические разработки (№ источника из списка литературы)
1	2	3	4	5
1	Лк.1	1 Основные понятия ИБ. 2 Угрозы безопасности информации, основные понятия: безопасность, конфиденциальность, целостность, доступность, утечка информации;	2	1,2, 3

		несанкционированный доступ к информации.		
2	Лк.2	1 Классификация угроз безопасности. 2 Прямые и косвенные каналы утечки данных.	2	1,8
3	Лк.3	1 Модель потенциального нарушителя. 2 Способы мошенничества в информационных системах.	2	1,5, 6, 8, 9, 11
4	Лк.4	1 Принципы организации систем обеспечения безопасности данных. 2 Требования, предъявляемые к системам обеспечения безопасности данных.	2	1,7
5	Лк.5	1 Понятие политики безопасности. 2 Гостехкомиссии в сфере обеспечения ИБ.	1	1,7
6	Лк.6	1 Принципы организации систем обеспечения безопасности данных. 2 Понятие мониторов безопасности.	2	1,2, 3
7	Лк.7	1 Руководящие документы Гостехкомиссии в сфере обеспечения ИБ. 2 Межсетевые экраны.	2	1,8
8	Лк.8	1 Типы компьютерных вирусов. 2 Методы борьбы с компьютерными вирусами.	2	1,5, 6, 8, 9, 11
9	Лк.9	1 Федеральный стандарт США на шифрование данных (стандарт DES). 2 Шифрование с открытым ключом, алгоритм RSA.	2	1,7
10	Лк.10	1 Средства построения защищённой виртуальной сети. 2 Туннелирование в протоколах различных уровней.	1	1,2, 3
		ИТОГО	**18**	

4.6Тематика для самостоятельной работы студентов

№ п/п	Тематика по содержанию дисциплины, выделенная для самостоятельного изучения	Количество часов из содержания дисциплины	Рекомендуемая литература и источники информации	Формы контроля СРС
1	2	3	4	5
1	1 Основные понятия ИБ. 2 Угрозы безопасности информации, основные понятия: безопасность, конфиденциальность, целостность, доступность, утечка информации; несанкционированный доступ к информации.	23	1,2,3,4	Отчет

2	1 Классификация угроз безопасности. 2 Прямые и косвенные каналы утечки данных.	23	Интернет, 10	Отчет
3	1 Модель потенциального нарушителя. 2 Способы мошенничества в информационных системах.	23	4,7,8	Отчет
4	1 Принципы организации систем обеспечения безопасности данных. 2 Требования, предъявляемые к системам обеспечения безопасности данных.	23	4,15	Отчет
5	1 Понятие политики безопасности. 2 Гостехкомиссии в сфере обеспечения ИБ.	23	1,2,11,12	Отчет
6	1 Принципы организации систем обеспечения безопасности данных. 2 Понятие мониторов безопасности.	23	Интернет , 1	Отчет
7	1 Руководящие документы Гостехкомиссии в сфере обеспечения ИБ. 2 Межсетевые экраны.	23	1, интернет	Отчет
8	1 Типы компьютерных вирусов. 2 Методы борьбы с компьютерными вирусами.	23	1, интернет	Отчет
9	1 Федеральный стандарт США на шифрование данных (стандарт DES). 2 Шифрование с открытым ключом, алгоритм RSA.	23	13, 4, 5	Отчет
10	1 Средства построения защищённой виртуальной сети. 2 Туннелирование в протоколах различных уровней.	26	14, 15, 5, 6	Отчет
	ИТОГО	**234**		

5.Образовательные технологии ______________________

При изучении дисциплины предусматривается использование в учебном процессе активных интерактивных форм проведения занятий в объеме 20% от аудиторной нагрузки.

При изучении дисциплины используются аудитории, оборудованные мультимедийными средствами обучения: проектором, ноутбуком, интерактивной доской.

Проведение лабораторных практикумов осуществляется в лабораториях, оснащенных лабораторным оборудованием:

лаборатории информационных технологий (аудитории: 306, 303);

лаборатория технических средств информатизации (аудитории: 308).

Использование интернет-ресурсов предполагает проведение занятий в компьютерных классах с выходом в Интернет. В компьютерных классах обучающиеся имеют доступ к информационным ресурсам, к базе данных библиотеки.

6.Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно2-методическое обеспечение самостоятельной работы студентов

ВОПРОСЫ ВХОДНОГО КОНТРОЛЯ

1.Основные понятия ИБ.

2.Информация,защищаемая информация, ценность информации, уровень секретности.

3.Объекты защиты информации.

4.Угрозы безопасности информации, основные понятия: безопасность, конфиденциальность, целостность, доступность, утечка информации; несанкционированный доступ к информации.

5.Классификация угроз безопасности: каналы утечки, воздействия.

6.Прямые и косвенные каналы утечки данных.
7. Основы теории ИБ
8.Модель потенциального нарушителя.
9.Способы мошенничества в информационных системах. 3.Основные способы реализации угроз ИБ.
10.Основные понятия теории ИБ.
11. Оценка эффективности систем защиты информации
12.Принципы организации систем обеспечения безопасности данных.
13.Требования, предъявляемые к системам обеспечения безопасности данных.
14. Понятие мониторов безопасности. 4.Физические средства защиты Информации

ПЕРЕЧЕНЬ ВОПРОСОВ ТЕКУЩИХ КОНТРОЛЬНЫХ РАБОТ

Аттестационная контрольная № 1

1.Основные понятия ИБ.
2.Информация,защищаемая информация, ценность информации, уровень секретности.
3.Объекты защиты информации.
4.Угрозы безопасности информации, основные понятия: безопасность, конфиденциальность, целостность, доступность, утечка информации; несанкционированный доступ к информации.
5.Классификация угроз безопасности: каналы утечки, воздействия.
6.Прямые и косвенные каналы утечки данных.
7. Основы теории ИБ
8.Модель потенциального нарушителя.
9.Способы мошенничества в информационных системах.
10.Основные способы реализации угроз ИБ.

Аттестационная контрольная № 2

1.Основные понятия теории ИБ.
2. Оценка эффективности систем защиты информации
3.Принципы организации систем обеспечения безопасности данных.
4.Требования, предъявляемые к системам обеспечения безопасности данных.
5. Понятие мониторов безопасности.
6.Физические средства защиты информации
7. Нормативные руководящие документы в сфере обеспечения ИБ

Аттестационная контрольная № 3

1. Понятие политики безопасности.
Дискреционные политики безопасности. Мандатные политики безопасности
2. Модель безопасности информационных потоков.
3.Показатели эффективности систем защиты информации.
4.Способы оценки эффективности систем защиты информации.
5.Руководящие документы Гостехкомиссии в сфере обеспечения ИБ

Вопросы к зачету по дисциплине «Информационная безопасность»

1.Основные понятия ИБ.
2.Информация,защищаемая информация, ценность информации, уровень секретности.
3.Объекты защиты информации.
4.Угрозы безопасности информации, основные понятия: безопасность, конфиденциальность, целостность, доступность, утечка информации; несанкционированный доступ к информации.
5.Классификация угроз безопасности: каналы утечки, воздействия.

6.Прямые и косвенные каналы утечки данных.
7. Основы теории ИБ
8.Модель потенциального нарушителя.
9.Способы мошенничества в информационных системах. 3.Основные способы реализации угроз ИБ.
10.Основные понятия теории ИБ.
11. Оценка эффективности систем защиты информации
12.Принципы организации систем обеспечения безопасности данных.
13.Требования, предъявляемые к системам обеспечения безопасности данных.
14. Понятие мониторов безопасности. 4.Физические средства защиты информации
15. Нормативные руководящие документы в сфере обеспечения ИБ
16. Понятие политики безопасности.
Дискреционные политики безопасности. Мандатные политики безопасности
17. Модель безопасности информационных потоков.
18.Показатели эффективности систем защиты информации.
19.Способы оценки эффективности систем защиты информации.
20.Руководящие документы Гостехкомиссии в сфере обеспечения ИБ

Вопросы к экзамену по дисциплине «Информационная безопасность»

1.Основные понятия ИБ.
2.Информация,защищаемая информация, ценность информации, уровень секретности.
3.Объекты защиты информации.
4.Угрозы безопасности информации, основные понятия: безопасность, конфиденциальность, целостность, доступность, утечка информации; несанкционированный доступ к информации.
5.Классификация угроз безопасности: каналы утечки, воздействия.
6.Прямые и косвенные каналы утечки данных.
7. Основы теории ИБ
8.Модель потенциального нарушителя.
9.Способы мошенничества в информационных системах. 3.Основные способы реализации угроз ИБ.
10.Основные понятия теории ИБ.
11. Оценка эффективности систем защиты информации
12.Принципы организации систем обеспечения безопасности данных.
13.Требования, предъявляемые к системам обеспечения безопасности данных.
14. Понятие мониторов безопасности. 4.Физические средства защиты информации
15. Нормативные руководящие документы в сфере обеспечения ИБ
16. Понятие политики безопасности.
Дискреционные политики безопасности. Мандатные политики безопасности
17. Модель безопасности информационных потоков.
18.Показатели эффективности систем защиты информации.
19.Способы оценки эффективности систем защиты информации.
20.Руководящие документы Гостехкомиссии в сфере обеспечения ИБ
21.Программно-технические средства обеспечения ИБ
22.Основные понятия теории ИБ.
23.Принципы организации систем обеспечения безопасности данных.
24.Требования, предъявляемые к системам обеспечения безопасности данных.
25.Понятие мониторов безопасности.
26.Физические средства защиты информации

27.Руководящие документы Гостехкомиссии в сфере обеспечения ИБ. «Общие критерии».
28.Структура. Основные понятия.
29.Программно-технические средства обеспечения ИБ.
30.Межсетевые экраны.
31.Борьба с компьютерными вирусами
32.Типы компьютерных вирусов.
33.Методы борьбы с компьютерными вирусами.
34. Криптографические методы
35.Федеральный стандарт США на шифрование данных (стандарт DES).
36.Отечественный стандарт шифрование данных.
37. Шифрование с открытым ключом, алгоритм RSA.
38.Построение защищённых виртуальных сетей
39.Понятие, назначение и основные функции защищённой виртуальной сети.
40.Средства построения защищённой виртуальной сети.
41.Туннелирование в протоколах различных уровней.

Тесты для проверки остаточных знаний
1) К правовым методам, обеспечивающим информационную безопасность, относятся:
- Разработка аппаратных средств обеспечения правовых данных
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий
+ Разработка и конкретизация правовых нормативных актов обеспечения безопасности
2) Основными источниками угроз информационной безопасности являются все указанное в списке:
- Хищение жестких дисков, подключение к сети, инсайдерство
+ Перехват данных, хищение данных, изменение архитектуры системы
- Хищение данных, подкуп системных администраторов, нарушение регламента работы
3) Виды информационной безопасности:
+ Персональная, корпоративная, государственная
- Клиентская, серверная, сетевая
- Локальная, глобальная, смешанная
4) Цели информационной безопасности – своевременное обнаружение, предупреждение:
+ несанкционированного доступа, воздействия в сети
- инсайдерства в организации
- чрезвычайных ситуаций
5) Основные объекты информационной безопасности:
+ Компьютерные сети, базы данных
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы
6) Основными рисками информационной безопасности являются:
- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети
+ Потеря, искажение, утечка информации
7) К основным принципам обеспечения информационной безопасности относится:
+ Экономической эффективности системы безопасности
- Многоплатформенной реализации системы
- Усиления защищенности всех звеньев системы
8) Основными субъектами информационной безопасности являются:
- руководители, менеджеры, администраторы компаний
+ органы права, государства, бизнеса
- сетевые базы данных, фаерволлы
9) К основным функциям системы безопасности можно отнести все перечисленное:
+ Установление регламента, аудит системы, выявление рисков
- Установка новых офисных приложений, смена хостинг-компании
- Внедрение аутентификации, проверки контактных данных пользователей
тест 10) Принципом информационной безопасности является принцип недопущения:
+ Неоправданных ограничений при работе в сети (системе)
- Рисков безопасности сети, системы

- Презумпции секретности
11) Принципом политики информационной безопасности является принцип:
+ Невозможности миновать защитные средства сети (системы)
- Усиления основного звена сети, системы
- Полного блокирования доступа при риск-ситуациях
12) Принципом политики информационной безопасности является принцип:
+ Усиления защищенности самого незащищенного звена сети (системы)
- Перехода в безопасное состояние работы сети, системы
- Полного доступа пользователей ко всем ресурсам сети, системы
13) Принципом политики информационной безопасности является принцип:
+ Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
- Одноуровневой защиты сети, системы
- Совместимых, однотипных программно-технических средств сети, системы
14) К основным типам средств воздействия на компьютерную сеть относится:
- Компьютерный сбой
+ Логические закладки («мины»)
- Аварийное отключение питания
15) Когда получен спам по e-mail с приложенным файлом, следует:
- Прочитать приложение, если оно не содержит ничего ценного – удалить
- Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
+ Удалить письмо с приложением, не раскрывая (не читая) его
16) Принцип Кирхгофа:
- Секретность ключа определена секретностью открытого сообщения
- Секретность информации определена скоростью передачи данных
+ Секретность закрытого сообщения определяется секретностью ключа
17) ЭЦП – это:
- Электронно-цифровой преобразователь
+ Электронно-цифровая подпись
- Электронно-цифровой процессор

7.Учебно-методическое и информационное обеспечение дисциплины

№ п/п	Виды занятий	Необходимая учебная, учебно-методическая (основная и дополнительная) литература, программное обеспечение и Интернет ресурсы	Автор(ы)	Издательство и год издания	Количество изданий	
					В библиотеке	На кафедре
Основная литература						
1	Лк Лб	Информационная безопасность : учебник и практикум для академического бакалавриата / С.А. Нестеров. — М. : Издательство Юрайт, 2018 — 321 с.	Нестеров, С. А.	— М.: Издательство Юрайт, 2018 — 321 с. — (Серия : Университеты России). — ISBN		
2	Лк Лб	Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры	Т.А. Полякова, А. А.Стрельцов, С. Г.Чубукова, В. А. Ниесов ; под ред. Т. А. Поляковой, А. А. Стрельцова..	— М. : Издательство Юрайт, 2018 — 325 с. — (Серия : Бакалавр и магистр. Академический курс). —		

3	Лк лб	Надежность и безопасность программного обеспечения : учеб. пособие для бакалавриата и магистратуры / О. В.Казарин, И. Б. Шубинский	Казарин, О. В.	— М. : Издательство Юрайт, 2018 — 342 с. — (Серия : Бакалавр и магистр. Модуль.). — ISBN 978-5-534-05142-1.		
Дополнительная литература						
4	Лк лб	Информатика (курс лекций) : учеб. пособие для вузов	Безручко, В. Т.	– Москва : Форум : Инфра-М, 2014 – 431 с.*		
5	Лк лб	Информатика : учебник для вузов	Гуриков, С. Р.	. – Москва : Форум, 2014 – 462 с.*		
6	Лк лб	Информатика : учебник для вузов / ред.– 2-е изд., испр. и доп.	В. В. Трофимов.	– Москва : Юрайт, 2013 – 916 с.*		
7	Лк лб	Информатика и программирование : учебник для вузов	Истомин, Е. П. Неклюдов, В. И. Романенко.	Андреевский издат. дом, 2006 – 248 с.*		
8	Лк лб	Основы современной информатики : учеб. пособие для вузов	Кудинов, Ю. И. Пащенко Ф. Ф..	Краснодар : Лань, 2011 – 255 с.*		
		Программное обеспечение и Интернет ресурсы				
		Лицензионный пакет программ MicrosoftWindows 7.				
		Электронная библиотечная система «IPRbooks» [Электронный ресурс]. – Электрон. дан. – Режим доступа : http://www.iprbookshop.ru/ Интернет университет информационных технологий [Электронный ресурс]. – Электрон. дан. –Режим доступа : http://www.intuit.ru/ 3 Учебный центр компьютерных технологий «Микроинформ» [Электронный ресурс]. – Электрон. дан. – Режим доступа : http://www.microinform.ru/ 4 Библиотека Genesis [Электронный ресурс].–Электрон.дан.–Режим доступа: http://gen.lib.rus.ec/ 5 Образовательный математический сайт [Электронный ресурс]. – Электрон. дан. – Режим доступа : http://www.exponenta.ru/ 6 Научная электронная библиотека [Электронный ресурс]. – Электрон.				

		дан. – Режим доступа : http://www.elibrary.ru/ Sustainability web — sites):				

Материально-техническое обеспечение дисциплины – Филиал располагает всем необходимым материально-техническим обеспечением для выполнения настоящей программы. Оно включает в себя:

- наличие компьютерного класса;
- наличие доступного для студента выхода в Интернет;
- наличие специально оборудованных кабинетов и аудиторий для мультимедийных презентаций.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению 09.03.03-«Прикладная информатика» с учетом рекомендаций примерной ООП ВО по профилю подготовки бакалавров 09.03.03.-«Прикладная информатика в экономике»

Рецензент от выпускающей кафедры (работодателя) по направлению
____________________ Б.М.Атаева
Подпись И.О.Ф

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ В РАБОЧЕЙ ПРОГРАММЕ НА 20___/20___ УЧЕБНЫЙ ГОД

В рабочую программу вносятся следующие изменения

____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____

Рабочая программа пересмотрена и одобрена
на заседании кафедры __________________ 20___

Зав. кафедрой ________________________________

Внесенные изменения утверждаю
Проректор по учебной работе (декан)_________________________

_______________________ 20____.