

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Баламирзоев Назим Лиодинович

Должность: Ректор

Дата подписания: 17.11.2025 16:52:08

Уникальный программный ключ:

043f149fe29b39f38c91fa342d88c83cd0d6921f

Министерство науки и высшего образования РФ

**Федеральное государственное бюджетное образовательное учреждение
высшего образования**

«Дагестанский государственный технический университет»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина «Информационная безопасность»
наименование дисциплины по ОПОП

для направления 09.03.03 – «Прикладная информатика»
код и полное наименование направления (специальности)

по профилю «Прикладная информатика в экономике»

факультет Филиал в г. Дербенте
наименование факультета, где ведется дисциплина

кафедра Естественных, гуманитарных, общепрофессиональных и
специальных дисциплин
наименование кафедры, за которой закреплена дисциплина

Форма обучения очная, заочная курс 4 семестр (ы) 7.
очная, очно-заочная, заочная

Программа составлена в соответствии с требованиями ФГОС ВО по направлению подготовки (специальности) 09.03.03 Прикладная информатика, с учетом рекомендаций и ОПОП ВО по направлению и профилю подготовки Прикладная информатика в экономике.

Разработчик

подпись

Е.Р. Джумалиева, ст. преподаватель
(ФИО уч. степень, уч. звание)

« 27 » сентября 2022 г.

Зав. кафедрой, за которой закреплена программа

С.Ф.Исмаилова, к.социол.н.

подпись

(ФИО уч. степень, уч. звание)

« 27 » сентября 2022 г.

Программа одобрена на заседании выпускающей кафедры ЕГОиСД от

« 27 » сентября 2022 года, протокол № 2

Зав. выпускающей кафедрой, по данному направлению (специальности, профилю)

С.Ф.Исмаилова, к.социол.н.

подпись

(ФИО уч. степень, уч. звание)

« 27 » сентября 2022 г.

Программа одобрена на заседании Методического совета филиала г.Дербенте от
« 28 » сентября 2022 года, протокол № 1

Председатель Методического совета филиала

Аликберов Н.А., к.ф.-м.н., ст.преподаватель

подпись

(ФИО уч. степень, уч. звание)

« 28 » сентября 2022 г.

СОГЛАСОВАНО:

Директор филиала

Мейланов

/ И.М.Мейланов/

подпись

Начальник УО

Магомаева Э.В.

подпись

Проректор по УР

Н.Л. Баламирзоев

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 обязательную часть УП (Б1.О.18)

3. Требования к уровню освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1. Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. ОПК-3.2. Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. ОПК-3.3. Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.
ОПК-4. Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	ОПК-4.1. Знает основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы. ОПК-4.2. Умеет применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы. ОПК-4.3. Владеет навыками составления технической документации на различных этапах жизненного цикла информационной системы.

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 организаций, 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 33ЕТ – 108час, в том числе – лекционные 17 часов, лабораторная работа 34 часов, СРС 57 часов, форма отчетности:7 семестр – зачет с оценкой

4.1. Содержание дисциплины.

№ п/п	Раздел дисциплины тема лекции и вопросы	Семестр	Недели 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	2		4	5	Входной контроль	
2	ЛЕКЦИЯ 2. Угрозы ИБ 1.Классификация угроз безопасности: каналы утечки, воздействия. 2.Прямые и косвенные каналы утечки данных.	1	5-7	2		4	5	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	2		4	5	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	2		4	6	Аттестационная работа №3	
5	ЛЕКЦИЯ 5. Нормативные руководящие документы в сфере обеспечения ИБ 1 Понятие политики безопасности. Дискреционные политики безопасности. Мандатные политики безопасности	1	17	2		4	6		

	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							
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	2		4	6	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	2		4	6	Аттестационная работа №1
8	ЛЕКЦИЯ 8. Борьба с компьютерными вирусами 1.Типы компьютерных вирусов. 2.Методы борьбы с компьютерными вирусами.	1	9-11	1		2	6	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	1		2	6	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	1		2	6	Посещение занятий, тесты.
Итого			17	17		34	57	зачет

4.2 Содержание лабораторных занятий

№ п/п	№ лекции из рабочей программы	Наименование (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.	4	1,2, 3
2	Лк.2	1 Классификация угроз безопасности. 2 Прямые и косвенные каналы утечки данных.	4	1,8
3	Лк.3	1 Модель потенциального нарушителя. 2 Способы мошенничества в информационных системах.	4	1,5, 6, 8, 9, 11
4	Лк.4	1 Принципы организации систем обеспечения безопасности данных. 2 Требования, предъявляемые к системам обеспечения безопасности данных.	4	1,7
5	Лк.5	1 Понятие политики безопасности. 2 Гостехкомиссии в сфере обеспечения ИБ.	4	1,7
6	Лк.6	1 Принципы организации систем обеспечения безопасности данных. 2 Понятие мониторов безопасности.	4	1,2, 3
7	Лк.7	1 Руководящие документы Гостехкомиссии в сфере обеспечения ИБ. 2 Межсетевые экраны.	4	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.	2	1,2, 3
		ИТОГО	34	

4.3 Тематика 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.	5	1,2,3,4	Отчет
2	1 Классификация угроз безопасности. 2 Прямые и косвенные каналы утечки данных.	5	Интернет, 10	Отчет
3	1 Модель потенциального нарушителя. 2 Способы мошенничества в информационных системах.	5	4,7,8	Отчет
4	1 Принципы организации систем обеспечения безопасности данных. 2 Требования, предъявляемые к системам обеспечения безопасности данных.	6	4,15	Отчет
5	1 Понятие политики безопасности. 2 Гостехкомиссии в сфере обеспечения ИБ.	6	1,2,11,12	Отчет
6	1 Принципы организации систем обеспечения безопасности данных. 2 Понятие мониторов безопасности.	6	Интернет, 1	Отчет
7	1 Руководящие документы Гостехкомиссии в сфере обеспечения ИБ. 2 Межсетевые экраны.	6	1, интернет	Отчет
8	1 Типы компьютерных вирусов. 2 Методы борьбы с компьютерными вирусами.	6	1, интернет	Отчет
9	1 Федеральный стандарт США на шифрование данных (стандарт DES). 2 Шифрование с открытым ключом, алгоритм RSA.	6	13, 4, 5	Отчет
10	1 Средства построения защищённой виртуальной сети. 2 Туннелирование в протоколах различных уровней.	6	14, 15, 5, 6	Отчет
ИТОГО		57		

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

Общая трудоемкость дисциплины составляет 33ЕТ – 108час, в том числе – лекционные 4 часов, лабораторная работа 9 часов, СРС 91 часов, форма отчетности:5 курс – зачет с оценкой

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 5								
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		1		1	9	
2	ЛЕКЦИЯ 2. Угрозы ИБ 1.Классификация угроз безопасности: каналы утечки, воздействия. 2.Прямые и косвенные каналы утечки данных.	4		1		1	9	
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				1	9	
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				1	9	
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	9	
6	ЛЕКЦИЯ 6. Программно-технические средства обеспечения ИБ	5		1		1	9	

	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	1		1	9	
8	ЛЕКЦИЯ 8. Борьба с компьютерными вирусами 1.Типы компьютерных вирусов. 2.Методы борьбы с компьютерными вирусами.	5			1	9	
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			1	9	
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	10	
Итого		5	4		9	91	зачет

4.5 Содержание лабораторных занятий

№ п/п	№ лекции из рабочей программы	Наименование (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	1	1,2, 3

		информации; несанкционированный доступ к информации.		
2	Лк.2	1 Классификация угроз безопасности. 2 Прямые и косвенные каналы утечки данных.	1	1,8
3	Лк.3	1 Модель потенциального нарушителя. 2 Способы мошенничества в информационных системах.	1	1,5, 6, 8, 9, 11
4	Лк.4	1 Принципы организации систем обеспечения безопасности данных. 2 Требования, предъявляемые к системам обеспечения безопасности данных.	1	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.	1	1,2, 3
7	Лк.7	1 Руководящие документы Гостехкомиссии в сфере обеспечения ИБ. 2 Межсетевые экраны.	1	1,8
8	Лк.8	1 Типы компьютерных вирусов. 2 Методы борьбы с компьютерными вирусами.	1	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.	1	1,7
10	Лк.10	1 Средства построения защищённой виртуальной сети. 2 Туннелирование в протоколах различных уровней.	1	1,2, 3
		ИТОГО	9	

4.6 Тематика 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.	9	1,2,3,4	Отчет

2	1 Классификация угроз безопасности. 2 Прямые и косвенные каналы утечки данных.	9	Интернет, 10	Отчет
3	1 Модель потенциального нарушителя. 2 Способы мошенничества в информационных системах.	9	4,7,8	Отчет
4	1 Принципы организации систем обеспечения безопасности данных. 2 Требования, предъявляемые к системам обеспечения безопасности данных.	9	4,15	Отчет
5	1 Понятие политики безопасности. 2 Гостехкомиссии в сфере обеспечения ИБ.	9	1,2,11,12	Отчет
6	1 Принципы организации систем обеспечения безопасности данных. 2 Понятие мониторов безопасности.	9	Интернет , 1	Отчет
7	1 Руководящие документы Гостехкомиссии в сфере обеспечения ИБ. 2 Межсетевые экраны.	9	1, интернет	Отчет
8	1 Типы компьютерных вирусов. 2 Методы борьбы с компьютерными вирусами.	9	1, интернет	Отчет
9	1 Федеральный стандарт США на шифрование данных (стандарт DES). 2 Шифрование с открытым ключом, алгоритм RSA.	9	13, 4, 5	Отчет
10	1 Средства построения защищённой виртуальной сети. 2 Туннелирование в протоколах различных уровней.	10	14, 15, 5, 6	Отчет
	ИТОГО	91		

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 од 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	Надежность и	Казарин, О. В.	— М. :		

	лб	безопасность программного обеспечения : учеб. пособие для бакалавриата и магистратуры / О. В.Казарин, И. Б. Шубинский		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. Пашенко Ф. Ф..	Краснодар : Лань, 2011 – 255 с.*		
		Программное обеспечение и Интернет ресурсы				
		Лицензионный пакет программ Microsoft Windows 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.

Специальные условия инвалидам и лицам с ограниченными возможностями здоровья (ОВЗ)

Специальные условия обучения и направления работы с инвалидами и лицами с ОВЗ определены на основании:

- Федерального закона от 29.12.2012 №273-ФЗ «Об образовании в Российской Федерации»;
- Федерального закона от 24.11.1995 № 181-ФЗ «О социальной защите инвалидов в Российской Федерации»;
- приказа Минобрнауки России от 05.04.2017 № 301 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры»;
- методических рекомендаций по организации образовательного процесса для обучения инвалидов и лиц с ограниченными возможностями здоровья в образовательных организациях высшего образования, в том числе оснащенности образовательного процесса, утвержденных Минобрнауки России 08.04.2014 № АК-44/05вн).

Практическая подготовка для обучающихся с ограниченными возможностями здоровья и инвалидов организуется с учетом особенностей их психофизического развития, индивидуальных возможностей и состояния здоровья.

Инвалиды и лица с ограниченными возможностями здоровья могут проходить практическую подготовку в организациях, где созданы специальные рабочие места или имеются возможности принятия таких обучающихся, с учетом рекомендации медико-социальной экспертизы относительно условий и видов труда.

Инвалиды и лица с ограниченными возможностями здоровья могут сдавать зачеты в сроки, установленные индивидуальным учебным планом. Инвалиды и лица с ограниченными возможностями здоровья, имеющие нарушения опорно-двигательного аппарата допускаются на аттестационные испытания в сопровождении ассистентов – сопровождающих.

Инвалиды и лица с ограниченными возможностями здоровья обязаны выполнить программу практик в рамках ОПОП/адаптированных ОПОП

9. Лист изменений и дополнений к рабочей программе

Дополнения и изменения в рабочей программе на 20____/20____учебный год.

В рабочую программу вносятся следующие изменения:

1.;
2.;
3.;
4.;
5.

или делается отметка о нецелесообразности внесения каких-либо изменений или дополнений на данный учебный год.

Рабочая программа пересмотрена и одобрена на заседании кафедры ЕГОиСД____ от
_____ года, протокол №_____

Заведующий кафедрой ЕГОиСД_____ Исмаилова С.Ф.
(название кафедры) (подпись, дата) (ФИО, уч. степень, уч. звание)

Согласовано:

Директор филиала _____ Мейланов И.М._____
(подпись, дата) (ФИО, уч. степень, уч. звание)
Председатель МС филиала _____ Аликберов Н.А., к.т.н._____
(подпись, дата) (ФИО, уч. степень, уч. звание)