Утверждено приказом ГОУ ВПО ДонГУУ от 23.08.2016г. №675

ДОНЕЦКАЯ НАРОДНАЯ РЕСПУБЛИКА
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«ДОНЕЦКАЯ АКАДЕМИЯ УПРАВЛЕНИЯ И ГОСУДАРСТВЕННОЙ СЛУЖБЫ
ПРИ ГЛАВЕ ДОНЕЦКОЙ НАРОДНОЙ РЕСПУБЛИКИ»

ФАКУЛЬТЕТ ГОСУДАРСТВЕННОЙ СЛУЖБЫ И УПРАВЛЕНИЯ
КАФЕДРА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

УТВЕРЖДАЮ
Проректор по учебной работе
_____ Л.Н.Костина
10.06.2017 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«Информационная безопасность»

Направление подготовки 09.03.03 «Прикладная информатика»

Донецк
2017

2

Рабочая программа учебной дисциплины «Информационная безопасность» для студентов 3 курса образовательного уровня «бакалавр» направления подготовки 09.03.03 «Прикладная информатика», для студентов очной и заочной форм обучения.

Автор,
разработчик: Доцент кафедры, к.т.н., доц., И.Л.Семичастный

Программа рассмотрена на
заседании ПМК кафедры «Прикладная информатика»

Протокол заседания ПМК от 08.06.2017 № 10

Председатель ПМК А. Н. Веряндов

Программа рассмотрена на
заседании кафедры Информационных технологий

Протокол заседания кафедры от 09.06.2017 № 13

Заведующая кафедрой Н. В. Брадул

Рабочая программа учебной дисциплины «Информационная безопасность» для студентов 3 курса образовательного уровня «бакалавр» направления подготовки 09.03.03 «Прикладная информатика», для студентов очной и заочной форм обучения.

Автор,
разработчик: Доцент кафедры, к.т.н., доц., И.Л.Семичастный

Программа рассмотрена на
заседании ПМК кафедры *«Прикладная информатика»*

Протокол заседания ПМК от 08.06.2017 № 10

Председатель ПМК _____ А. Н. Верзилов

Программа рассмотрена на
заседании кафедры *Информационных технологий*

Протокол заседания кафедры от 09.06.2017 № 13

Заведующая кафедрой _____ Н. В. Брадул

1. Цель освоения дисциплины и планируемые результаты обучения по дисциплине (соотнесенные с планируемыми результатами освоения образовательной программы)

Цель изучения дисциплины – сформировать знания о принципах и способах противодействия опасностям и угрозам, возникающим в процессе развития современного информационного общества в сфере информационной безопасности.

Задачи учебной дисциплины:

- ознакомить студентов с современными технологиями, применяемыми в решении задач информационной безопасности, моделями возможных угроз, нормативными документами, терминологией и основными понятиями теории защиты информации;
- приобрести практические навыки анализа и выбора методов и средств защиты компьютерной информации.

Компетенции обучающегося, формируемые в результате освоения дисциплины:

Код соответствующей компетенции по ГОС	Наименование компетенций	Результат освоения (знать, уметь, владеть)
ОПК-1	способностью использовать нормативно-правовые документы, международные и отечественные стандарты в области информационных систем и технологий	**Знать:** - нормативные правовые документы в сфере информационной безопасности в области информационных систем и технологий. **Уметь:** - использовать нормативные правовые документы в сфере информационной безопасности в области информационных систем и технологий для организации защиты информации. **Владеть:** - международными и отечественными стандартами в области обеспечения безопасности информационных систем и технологий.
ОПК-3	способностью использовать основные законы естественнонаучных дисциплин и современные информационно-коммуникационные технологии в профессиональной деятельности	**Знать:** - основы защиты информации. **Уметь:** - реализовывать мероприятия для обеспечения на предприятии (в организации) деятельности в области защиты информации. **Владеть:**

		- навыками работы с методами и типовыми средствами защиты информации в вычислительных системах и сетях.
ОПК-4	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**Знать:** - виды угроз ИС и методы обеспечения информационной безопасности. **Уметь:** - применять методы анализа прикладной области на концептуальном, логическом, и алгоритмическом уровнях с целью выявления угроз безопасности. **Владеть:** - способностью блокировать угрозы безопасности ИС предприятия с помощью методов обеспечения защиты информации.
ПК-7	способностью эксплуатировать и сопровождать ИС и сервисы	**Знать:** - принципы эксплуатации и сопровождения информационных систем и сервисов с точки зрения обеспечения защиты от вредоносного ПО. **Уметь:** - эксплуатировать и сопровождать информационные системы и сервисы с точки зрения их защиты от вредоносного ПО. **Владеть:** - принципами эксплуатации и сопровождения информационных систем и сервисов с точки зрения их защиты от вредоносного ПО.
ПК-10	способностью принимать участие в организации ИТ-инфраструктуры в управлении	**Знать:** - типовые программно-аппаратные средства и системы зашиты

	информационной безопасностью	информации от несанкционированного доступа в компьютерную среду. **Уметь:** - использовать типовые программно-аппаратные средства и системы зашиты информации от несанкционированного доступа в компьютерную среду. **Владеть:** - навыками работы с методами и типовыми средствами защиты информации в вычислительных системах и сетях.
ППК-12	способностью осуществлять и обосновывать выбор проектных решений по видам обеспечения информационных систем	**Знать:** - принципы и методы разработки политики безопасности на предприятии. **Уметь:** - разрабатывать документы определяющие политику безопасности на предприятии. **Владеть:** - технологиями разработки и реализации политики безопасности на предприятии.

2. Место дисциплины в структуре основной образовательной программы

Дисциплина «Информационная безопасность» относится к базовой части дисциплин профессионального цикла учебного плана по направлению подготовки 09.03.03 «Прикладная информатика».

2.1. Требования к предварительной подготовке обучающегося

Дисциплина тесно связана с такими курсами, как: «Базы данных», «Теория систем и системный анализ», «Вычислительные системы, сети и телекоммуникации».

2.2. Дисциплины и/или практики, для которых освоение данной дисциплины необходимо как предшествующее:

Основные положения дисциплины могут быть использованы в дальнейшем при изучении следующих дисциплин: «Управление информационными системами», «Проектирование информационных систем», «Информационный менеджмент» и др.

3. Объем дисциплины в кредитах (зачетных единицах) с указанием количества

академических часов, выделенных на аудиторную (по видам учебных занятий) и самостоятельную работу студента

	Зачетные единицы (кредиты ECTS)	**Всего часов**	**Форма обучения**	
			Очная	
			Семестр	
			№5	**№6**
Общая трудоемкость	**5**	**180**	**Количество часов на вид работы:**	
Виды учебной работы, из них:				
Аудиторные занятия (всего)		**82**	**54**	**28**
В том числе:				
Лекции		**50**	**36**	**14**
Практические занятия		**32**	**18**	**14**
Самостоятельная работа (всего)		**98**	**49**	**49**
Промежуточная аттестация				
В том числе:				
экзамен			экзамен	экзамен

	Зачетные единицы (кредиты ECTS)	**Всего часов**	**Форма обучения**	
			Заочная	
			Семестр	
			№5	**№6**
Общая трудоемкость	**5**	**180**	**Количество часов на вид работы:**	
Виды учебной работы, из них:				
Аудиторные занятия (всего)		**14**	**6**	**8**
В том числе:				
Лекции		**6**	**2**	**4**
Практические занятия		**8**	**4**	**4**
Самостоятельная работа (всего)		**130**	**83**	**83**
Промежуточная аттестация				
В том числе:				
экзамен			экзамен	экзамен

4. Содержание дисциплины, структурированное по разделам (темам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Разделы (темы) дисциплины с указанием отведенного на них количества академических часов и видов учебных занятий

Наименование раздела, темы дисциплины	Виды учебной работы (бюджет времени) (вносятся данные по реализуемым формам)									
	Очная форма обучения					Заочная форма обучения				
	Лекции	Практические занятия	Семинарские занятия	Самостоятельная работа	Всего	Лекции	Практические занятия	Семинарские занятия	Самостоятельная работа	Всего
1	2	3	4	5	6	7	8	9	10	11
Раздел 1. Техноло-гии и методы обеспечения ИБ										
Тема 1.1. Основные понятия ИБ. ИБ в системе национальной безопасности России .	2	2		2	6	2	2		4	8
Тема 1.2. Информационные отношения, субъекты информационных отношений, их интересы, пути нанесения ущерба	2	2		2	6				4	4
Тема 1.3. Угрозы информационной безопасности .	2	2		2	6		2		4	6
Тема 1.4. Политика безопасности и формирование организационной структуры системы защиты информации на предприятии	2	2		2	6				4	4
Тема 1.5. Технологии защиты от вредоносных программ и спама.	2	2		2	6				4	4
Тема 1.6. Направления обеспечения ИБ. Правовая, информационная, техническая безопасность.	2	2		2	6				4	4
Тема 1.7. Защита от утечек по техническим каналам. Защита ИС и СВТ от средств электромагнитного воздействия	2	0,5		2	4,5				4	4

Наименование раздела, темы дисциплины	Виды учебной работы (бюджет времени) (вносятся данные по реализуемым формам)									
	Очная форма обучения					Заочная форма обучения				
	Лекции	Практические занятия	Семинарские занятия	Самостоятельная работа	Всего	Лекции	Практические занятия	Семинарские занятия	Самостоятельная работа	Всего
1	2	3	4	5	6	7	8	9	10	11
Тема 1.8. Основные принципы и методы в области технической защиты информации	2	0,5		2	4,5				4	4
Тема 1.9. Противодействие несанкционированному доступу к конфиденциальной информации	2	0,5		2	4,5				4	4
Тема 1.10. Критерии защищенности компьютерных систем. Лицензирование и сертификация ИБ.	2	0,5		2	4,5				4	4
Тема 1.11. Международные стандарты ИБ. COBIT	2	0,5		2	4,5				4	4
Тема 1.12. Практичес-кие аспекты безопасности ИС	2	0,5		2	4,5				4	4
Тема 1.13. Обеспечение безопасности ОС. Безопасность Windows 7	2	0,5		2	4,5				4	4
Тема 1.14. Криптографические методы защиты информации. Классификация криптографических методов защиты.	2	0,5		2	4,5				4	4
Тема 1.15. Симметричные криптографические алгоритмы	2	0,5		2	4,5				4	4
Тема 1.16. Асимметричные криптографические алгоритмы	2	0,5		3	5,5				4	4

Наименование раздела, темы дисциплины	Виды учебной работы (бюджет времени) (вносятся данные по реализуемым формам)									
	Очная форма обучения					Заочная форма обучения				
	Лекции	Практические занятия	Семинарские занятия	Самостоятельная работа	Всего	Лекции	Практические занятия	Семинарские занятия	Самостоятельная работа	Всего
1	2	3	4	5	6	7	8	9	10	11
Тема 1.17. Цифровая электронная подпись (ЭЦП).	2	0,5		3	5,5				4	4
Тема 1.18. Технологии аутентификации.	2	0,5		13	15,5				15	15
Итого по разделу:	**36**	**18**		**49**	**103**	**2**	**4**		**83**	**89**
Раздел 2. Информационная безопасность ИС и сетей										
Тема 2.1. Проблемы информационной безопасности сетей	2	2		5	9	2	2		10	14
Тема 2.2 Угрозы и уязвимости проводных корпоративных сетей	2	2		5	9	2	2		10	14
Тема 2.3. Технология защиты межсетевого обмена данными. Брандмауэры.	2	2		5	9				10	10
Тема 2.4. Технологии VPN.	2	2		6	10				10	10
Тема 2.5. ИБ в сетях. Интернет безопасность Стек протоколов TCP/IP	2	2		6	10				10	10
Тема 2.6. Защита информации в компьютерных сетях. Защита на канальном и сеансовом уровне.	2	2		6	10				10	10
Тема 2.7. Защита на сетевом уровне — протокол IPSec. Инфраструктура защиты на прикладном уровне	2	2		16	10				23	23
Итого по разделу:	**14**	**14**		**49**	**77**	**4**	**4**		**83**	**91**
Всего за семестр:	**50**	**32**		**98**	**180**	**6**	**8**		**166**	**180**

4.2. Содержание разделов дисциплины:

Наименование раздела, темы дисциплины	Содержание разделов дисциплины	Содержание семинарских/практических занятий	Кол-во часов	
			о	з
1	2	3	4	5
Раздел 1. Техноло-гии и методы обеспечения ИБ				
Тема 1.1.	Основные понятия ИБ. ИБ в системе национальной безопасности России .	**Практическое занятие №1**	**2**	**1**
		Основные категории ИБ. Подбор пароля.	2	1
Тема 1.2.	Информационные отношения, субъекты информационных отношений, их интересы, пути нанесения ущерба	**Практическое занятие №2**	**2**	**1**
		Основные категории ИБ. Программа TrueCrypt	2	1
Тема 1.3.	Угрозы информационной безопасности.	**Практическое занятие №3**	**2**	**1**
		Задачи обеспечения национальной ИБ	2	1
Тема 1.4.	Политика безопасности и формирование организационной структуры системы защиты информации на предприятии	**Практическое занятие №4**	**2**	**1**
		Классификация угроз безопасности на предприятии	2	1
Тема 1.5.	Технологии защиты от вредоносных программ и спама	**Практическое занятие №5**	**2**	
		Сравнительный анализ антивирусных пакетов	2	
Тема 1.6.	Направления обеспечения ИБ. Правовая, информационная, техническая безопасность.	**Практическое занятие №6**	**2**	
		Правовая защита ИБ	2	
Тема 1.7.	Защита ИС и СВТ от средств электромагнитного воздействия.	**Практическое занятие №7**	**0,5**	
		Программная защита ИБ	0,5	
Тема 1.8.	Основные принципы и методы в области технической защиты информации	**Практическое занятие №8**	**0,5**	
		Техническая защита ИБ	0,5	
Тема 1.9.	Противодействие несанк-ционированному доступу к конфиденциальной информации	**Практическое занятие №9**	**0,5**	
		Защита информации от НСД	0,5	
Тема 1.10.	Критерии защищенности ком-пьютерных систем. Лицензирование и сертификация ИБ.	**Практическое занятие №10**	**0,5**	
		Проверка режимов безопасности ОС, ПК и сети	0,5	
Тема 1.11.	Международные стандарты ИБ.	**Практическое занятие**	**0,5**	

Наименование раздела, темы дисциплины	Содержание разделов дисциплины	Содержание семинарских/практических занятий		
			Кол-во часов	
			о	з
1	2	3	4	5
	COBIT	**№11**		
		Проверка режимов безопасности ОС, ПК и сети	0,5	
Тема 1.12.	Практические аспекты безопасности ИС	**Практическое занятие №12**	**0,5**	
		Проверка режимов безопасности ПК	0,5	
Тема 1.13.	Обеспечение безопасности ОС. Безопасность Windows 7	**Практическое занятие №13**	**0,5**	
		Проверка режимов безопасности ПК	0,5	
Тема 1.14.	Криптографические методы защиты информации. Классификация криптографических методы защиты.	**Практическое занятие №14**	**0,5**	
		Криптографические методы защиты информации	0,5	
Тема 1.15.	Симметричные криптографические алгоритмы	**Практическое занятие №15**	**0,5**	
		Шифрование данных алгоритмом Виженера	0,5	
Тема 1.16.	Асимметричные криптографические алгоритмы	**Практическое занятие №16**	**0,5**	
		Шифрование данных алгоритмом Виженера	0,5	
Тема 1.17.	Цифровая электронная подпись (ЭЦП).	**Практическое занятие №17**	**0,5**	
		Шифрование данных алгоритмом Виженера	0,5	
Тема 1.18.	Технологии аутентификации.	**Практическое занятие №18**	**0,5**	
		Асимметричные алгоритмы шифрования. NetShark	0,5	
Раздел 2. Информационная безопасность ИС и сетей				
Тема 2.1.	Проблемы информационной безопасности сетей	**Практическое занятие №19**	**2**	**2**
		Асимметричные алгоритмы шифрования. NetShark	2	2
Тема 2.2.	Угрозы и уязвимости проводных корпоративных сетей	**Практическое занятие №20**	**2**	**2**
		Проектирование файервола. Cisco Packet	2	2

Наименование раздела, темы дисциплины	Содержание разделов дисциплины	Содержание семинарских/практических занятий		
			Кол-во часов	
			о	з
1	2	3	4	5
		Tracer		
Тема 2.3.	Технология защиты межсетевого обмена данными. Брандмауэры	**Практическое занятие №21**	**2**	
		Проектирование файервола. Cisco Packet Tracer	2	
Тема 2.4.	Технологии VPN.	**Практическое занятие №22**	**2**	
		Проблемы сетевой безопасности. Применение технологии VPN	2	
Тема 2.5.	ИБ в сетях. Интернет безопасность Стек протоколов TCP/IP.	**Практическое занятие №23**	**2**	
		Проблемы сетевой безопасности. Применение технологии VPN	2	
Тема 2.6.	Защита информации в компьютерных сетях. Защита на канальном и сеансовом уровне.	**Практическое занятие №24**	**2**	
		Шифрование и электронно-цифровая подпись в системе документооборота. Программа PGP	2	
Тема 2.7.	Защита на сетевом уровне — протокол IPSec	**Практическое занятие №25**	**2**	
		Шифрование и электронно-цифровая подпись в системе документооборота. Программа PGP	2	

5. Перечень учебной литературы, необходимой для освоения дисциплины

5.1. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Элементы учебно-методического комплекса дисциплины утверждены на заседании кафедры информационных технологий (протокол №1 от 29.08.2017).

Методические указания к 8-и практическим работам по дисциплине и электронные варианты 25-ти лекций дисциплины и презентаций к ним выставлены в системе Moodle по адресу http://elearn.dsum.org/enrol/index.php?id=14 .

Каждая практическая работа содержит перечень контрольных вопросов для

самостоятельной работы студентов, а также список источников литературы и ссылок ресурсов глобальной сети.

Контрольные вопросы для самоподготовки для экзаменов:

Семестр 1

1. Информационная война как угроза информационной безопасности национального уровня
2. Объекты и субъекты информационного пространства. Примеры.
3. Субъекты информационных отношений и их интересы.
4. Три уровня управления политикой безопасности на предприятии.
5. Варианты построения виртуальных защищенных каналов.
6. Понятие «модели злоумышленника». Привести примеры.
7. Конфиденциальность информации. Способы обеспечения конфиденциальности информации в организации.
8. Практические методы аутентификации, используемые в настоящее время
9. Классификация каналов проникновения в систему и утечки информации
10. Политика информационной безопасности организации.
11. Содержание политики безопасности организации.
12. Определение информационной безопасности и ее составляющие.
13. Причины роста компьютерной преступности. Компьютерные преступления против государственных и общественных интересов.
14. Ключевые категории (понятия) безопасности и их взаимосвязь в соответствии с ГОСТ Р ИСО/МЭК 15408-1-2008.
15. Классификация вредоносных программ.
16. Сигнатурные методы обнаружения вредоносного ПО.
17. Проактивные методы обнаружения вредоносного ПО.
18. Тенденции развития современных антивирусных программ
19. Модули и режимы работы современных антивирусных программ.
20. Модель автоматизированной системы (ИС) и типы вирусных угроз безопасности ИС для ее различных уровней.
21. Защита периметра сети ИС предприятия с помощью межсетевых экранов (МСЭ)
22. Защита ИС предприятия на уровне рабочих станций пользователей и серверов.
23. Модель нарушителя антивирусной безопасности. Рекомендуемые методы защиты для классов нарушителей.
24. Тенденции развития современных антивирусных программ
25. Защита информации на уровне корпоративной сети предприятия.
26. Технические каналы утечки информации. Защита от утечек информации по техническим каналам
27. Модули и режимы работы современных антивирусных программ.
28. Модель автоматизированной системы (ИС) и типы вирусных угроз безопасности ИС для ее различных уровней.
29. Защита ИС предприятия на уровне рабочих станций пользователей и серверов.
30. Модель нарушителя антивирусной безопасности. Рекомендуемые методы защиты для классов нарушителей.
31. Защита информации на уровне корпоративной сети предприятия.
32. Методика создания демилитаризованных зон в корпоративной сети предприятия
33. Защита информации от утечки по электромагнитным каналам
34. Технические каналы утечки информации. Защита от утечек информации по техническим каналам
35. Направления обеспечения ИБ предприятия. Правовая и организационная защита.
36. Технология обеспечения безопасности ИС при беспроводном соединении

Семестр 2

1. Направления обеспечения ИБ предприятия. Физические и организационно-технические средства защиты.
2. Система обнаружения и предотвращения вторжений.
3. Технологии обеспечения безопасности в ОС Windows 7.
4. Способы защиты информации в организации. Характеристика защитных действий
5. Защита информации от утечки по визуально оптическим каналам.
6. Способы защиты информации в организации. Характеристика защитных действий
7. Направления обеспечения ИБ предприятия. Правовая и организационная защита.
8. Технология обеспечения безопасности ИС при беспроводном соединении
9. Система обнаружения и предотвращения вторжений.
10. Технологии обеспечения безопасности в ОС Windows 7.
11. Направления обеспечения ИБ предприятия. Физические и организационно-технические средства защиты.
12. Защита информации от утечки по электромагнитным каналам
13. Информационная безопасность на базе стандарта CobiT
14. Термины и определения криптографии.
15. Классификация криптографических алгоритмов
16. Критерии безопасности компьютерных систем «Оранжевая книга».
17. Криптографический алгоритм Виженера. Преимущества и недостатки.
18. Технологии биометрической аутентификации пользователя.
19. Преимущества и недостатки симметричных алгоритмов шифрования
20. Проблемы безопасности IP-сетей
21. Порядок использования систем с симметричными ключами.
22. Технологии строгой аутентификации пользователя.
23. Симметричные алгоритмы шифрования. Примеры
24. Структура и функциональность стека протоколов TCP/IP с точки зрения информационной безопасности.
25. Технология использование электронной цифровой подписи.
26. Классификация механизмов аутентификации пользователей
27. Классификация сетей VPN. Преимущества применения технологий VPN.
28. Структура политики безопасности организации
29. Преимущества и недостатки асимметричных систем шифрования.
30. Технологии виртуальных защищенных сетей (VPN). Основные понятия и функции сети VPN
31. Порядок использования систем с асимметричными ключами
32. Протоколы формирования защищенных каналов сети VPN на сеансовом уровне
33. Проблема целостности информации. Примеры нарушения целостности информации
34. Основные варианты архитектуры VPN. Средства обеспечения безопасности VPN.
35. Методы защиты информации на канальном и сеансовом уровнях.
36. Методы защита информации на сетевом уровне. Протокол IPSec

Указывается список учебно-методических материалов, которые помогают обучающемуся организовать самостоятельное изучение тем (вопросов) дисциплины.

Приводится **перечень собственных материалов**, к которым студент имеет возможность доступа, с указанием выходных данных учебников, электронных учебно-методических, учебных пособий и иных учебно-методических материалов, **выпущенных преподавателями**.

Для самостоятельного освоения дисциплины в обязательном порядке студентам предлагается перечень контрольных вопросов для самоподготовки.

5.2. Перечень основной учебной литературы

1. Галатенко В.А. Основы информационной безопасности [Электронный ресурс] / Галатенко В.А. – М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. – 266 с. – Режим доступа: http://www.iprbookshop.ru/52209 .
2. Гатчин Ю.А. Теория информационной безопасности и методология защиты информации [Электронный ресурс]: учебное пособие / Ю.А. Гатчин, В.В. Сухостат. – СПб.: СПбГУ ИТМО, 2010. – 98 с. Режим доступа: http://window.edu.ru/resource/984/71984/files/itmo477.pdf
3. Зайцев А.П. Технические средства и методы защиты информации: учебник для вузов [Электронный ресурс] / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО "Издательство Машиностроение", 2009. – 508 с. – Режим доступа: http://window.edu.ru/resource/611/63611/files/tsmzi.pdf
4. Скрипник Д.А. Общие вопросы технической защиты информации [Электронный ресурс] / Д.А. Скрипник – М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2012. – 264 с. – Режим доступа: http://www.intuit.ru/studies/courses/2291/591/info
5. Макаренко С.И. Информационная безопасность: Учебное пособие для студентов вузов [Электронный ресурс]. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 371 с. – Режим доступа: http://window.edu.ru/catalog/pdf2txt/775/77775/58783
6. Информация и безопасность. Журнал кафедры «Систем информационной безопасности» Воронежского государственного технического университета,. Ежеквартальное издание, включен в перечень ВАК РФ [Электронный ресурс]. – Режим доступа: http://elibrary.ru/title_about.asp?id=8748.
7. Вопросы кибербезопасности**.** Ежеквартальное издание, включен в перечень ВАК РФ [Электронный ресурс]. – Режим доступа: http://cyberrus.com/
8. Гатчин Ю.А., Сухостат В.В. Теория информационной безопасности и методология защиты информации. - СПб.: СПбГУ ИТМО, 2010. - 98 с.
9. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. – М., ИНРА-М, 2011. – 416 с.
10. Сычев В.Ю. Основы информационной безопасности. Учебно-практическое пособие. М.: Изд. центр ЕАОИ, 2007. – 300 с.
11. А.А. Малюк, С.В. Пазизин, Н.С. Погожин. Введение в защиту информации в автоматизированных системах: Учебное пособие для вузов - 4-е изд., стереотип. - М.: Горячая линия - Телеком, 2011.
12. Сычев Ю.Н. Основы информационная безопасность. Учебно-практическое пособие. – М.: Изд. центр ЕАОИ, 2007. – 300 с.
13. Ярочкин В.И. Информационная безопасность: Учеб. для вузов. М.: Академический проект, 2008. 544 с.

5.3. Перечень дополнительной литературы

1. Баскаков И.В., Евсеев В.Л., Пролетарский А.В., Суровов А.М. Защита информации в информационных системах: Учебное пособие. М.: 2011. 362 с.
2. Владимир Бройдо, Ольга Ильина. Вычислительные системы, сети и телекоммуникации: учебник для вузов (4-е издание). издательство "Питер". 2010 г. 560 стр.
3. Серия «Вопросы управления информационной безопасностью. Выпуск 1». - М.: Горячая линия - Телеком, 2014 г.
4. Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. - М.: Книжный мир, 2009. - 352 с.
5. Мещеряков Р.В., Шелупанов А.А., Белов Е.Б., Лось В.П. Основы информационной безопасности. – М.: Горячая линия – Телеком, 2006. – 540 с.

6. Скрипник Д.А. Общие вопросы технической защиты информации [Электронный ресурс]/ Скрипник Д.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2012.— 264 c.
7. Гатчин Ю.А. Основы информационной безопасности: учебное пособие/ Ю.А. Гатчин, Е.В. Климова. – СПб.: СПбГУ ИТМО, 2009. – 84с.

6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. https://cybermap.kaspersky.com/
2. http://freeprotection.ru/
3. http://www.itrn.ru/tag/?id=12
4. http://www.securitylab.ru/
5. http://www.e-uni.ee/e-kursused/itturvalisus_vk/index.html
6. http://www.itexpert.ru
7. http://www.sbcinfo/index.htm
8. http://www.infoforum.ru/
9. http://www.st-s.su
10. http://www.cnews.ru/
11. http://www.cryptography.ru/
12. https://www.opswat.com/resources/reports/antivirus-and-compromised-device-january-2015
13. http://www.matousec.com
14. http://www.pgpru.com/
15. http://dsec.ru/

7. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

7.1. Перечень информационных технологий (*при необходимости*)

При изучении дисциплины используются информационные технологии противодействия вредоносному ПО и спаму. Для этого используются следующие демонстрационные версии и свободнораспространяемые пакеты антивирусных программ: Avast, Microsoft Essentials, AVG, Avira, , Dr Web, ESET, Kaspersky Antivirus 2015, Kaspersky Internet Security, Comodo Internet Security, Spybot, Bitdefender, 360Total Security, Symantec Endpoint Protection, McAfee, Panda Security.

Кроме того при изучении технологий криптографии используется компьютерные программы PGP и TrueCrypt, а также библиотека функций, позволяющие выполнять операции шифрования и цифровой подписи сообщений, файлов и другой информации, представленной в электронном виде, в том числе прозрачное шифрование данных на запоминающих устройствах, например, на жёстком диске.

При изучении технологий VPN (Virtual Private Network) используется программа LogMeIn Hamachi.

7.2. Перечень программного обеспечения (*при необходимости*)

При изучении дисциплины используется ПО в составе пакета OS MS Windows, MS Office.

7.3. Перечень информационных справочных систем *(при необходимости)*

В процессе изучения дисциплины используются возможности информационно-справочной системы портала http://window.edu.ru/.

8. Фонд оценочных средств для контроля уровня сформированности компетенций

8.1. Виды промежуточной аттестации.

Текущий контроль успеваемости позволяет оценить уровень сформированности элементов компетенций (знаний и умений), компетенций с последующим объединением оценок и проводится в форме устного опроса (фронтальный, индивидуальный, комплексный), письменной проверки (контрольные, индивидуальные работы), включая задания для самостоятельной работы за компьютером.

Промежуточная аттестация в форме экзамена позволяет оценить уровень сформированности компетенций в целом по дисциплине и может осуществляться как в письменной так и в устной форме.

Темы рефератов:

1. Основные принципы организации защиты информации от НСД и обеспечения ее конфиденциальности.
2. Автоматизация процесса обработки конфиденциальной информации.
3. Стандарты информационной безопасности и их роль.
4. Угрозы безопасности компьютерных систем.
5. Механизм идентификации и аутентификации пользователей.
6. Конкретные мероприятия по обеспечению информационной безопасности и индивидуальные обязанности должностных лиц по выполнению этих требований.
7. Воздействия программных закладок на компьютеры.
8. Контроль доступа к библиотекам исходных текстов программ.
9. Политика информационной безопасности.
10. Права интеллектуальной собственности и обеспечение информационной безопасности.
11. Структура планов обеспечения непрерывности бизнеса.
12. Реализация механизмов безопасности на системном уровне.
13. Электронные подписи в электронной торговле.
14. Специальные меры противодействия компрометации служебной информации при использовании переносных устройств.
15. Средства защиты в составе вычислительной системы и управление ими.
16. Управление криптографическими ключами и хранение ключевой
17. информации.
18. Распределение криптографических ключей с участием центра распределения ключей.

Критерии оценки реферата

Оценка 5 ставится, если выполнены все требования к написанию и защите реферата: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы.

Оценка 4 – основные требования к реферату и его защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём реферата; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы.

Оценка 3 – имеются существенные отступления от требований к реферированию. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании реферата или при ответе на дополнительные вопросы; во время защиты отсутствует вывод.

Оценка 2 – тема реферата не раскрыта, обнаруживается существенное непонимание проблемы.
Оценка 1 – реферат не представлен.

8.2. Показатели и критерии оценки результатов освоения дисциплины.

Средним баллом за дисциплину является средний балл за текущую учебную деятельность.

Механизм конвертации результатов изучения студентом дисциплины в оценки по традиционной (государственной) шкале и шкале ECTS представлен в таблице.

Средний балл по дисциплине (текущая успеваемость)	**Отношение полученного студентом среднего балла по дисциплине к максимально возможной величине этого показателя**	**Оценка по государственной шкале**	**Оценка по шкале ECTS**	**Определение**
4,5 –5,0	90% – 100%	5	A	отлично – отличное выполнение с незначительным количеством неточностей (до 10%)
4,0 – 4,49	80% – 89%	4	B	хорошо – в целом правильно выполненная работа с незначительным количеством ошибок (до 20%)
3,75 – 3,99	75% – 79%	4	C	хорошо – в целом правильно выполненная работа с незначительным количеством ошибок (до 25%)
3,25 – 3,74	65% – 74%	3	D	удовлетворительно – неплохо, но со значительным количеством недостатков (до 35%)
3,0 – 3,24	60% – 64%	3	E	достаточно – выполнение удовлетворяет минимальные критерии, но со значительным количеством недостатков (до 40%)
до 3,0	35% – 59%	2	FX	неудовлетворительно с возможностью

				повторной сдачи (ошибок свыше 40%)
	0 – 34%	2	F	неудовлетворительно – надо поработать над тем, как получить положительную оценку (ошибок свыше 65%)

8.3. Критерии оценки работы студента.

При усвоении каждой темы за текущую учебную деятельность студента выставляются оценки по 5-балльной (государственной) шкале. Оценка за каждое задание в процессе текущей учебной деятельности определяется на основе процентного отношения операций, правильно выполненных студентом во время выполнения задания:

- 90-100% – «5»,
- 75-89% – «4»,
- 60-74% – «3»,
- менее 60% – «2».

Если на занятии студент выполняет несколько заданий, оценка за каждое задание выставляется отдельно.

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

Раздел 1. Технологии и методы обеспечения ИБ
Тема 1.1. Основные понятия ИБ. ИБ в системе национальной безопасности России

В качестве материала для оценки знаний студентов разработаны тесты этой теме

1. Информационный объект – это:
   a) аппаратная часть информационной инфраструктуры, хранящая данные;
   b) файлы (документы), ресурсы локальных и глобальных сетей;
   c) среда, в которой информация создается, передается, обрабатывается или хранится;
   d) файлы (документы), сайты, порталы, средства их создания .

2. Является ли информационное общество реализацией экономического и технологического уклада?
   a) да;
   b) нет;

3. Информационное общество — это общество, в котором:
   a) большинство работающих занято производством, хранением, переработкой и реализацией информации, особенно высшей её формы — знаний;
   b) постоянно растет количество интернет-пользователей;
   c) реализованы технологии электронного управления и электронного правительства;
   d) электронная коммерция является преобладающей экономической моделью.

4. *Основными компонентами информационного пространства являются*
   a) пользователи, информационные ресурсы, провайдеры;
   b) владельцы, провайдеры, информационная инфраструктура;

c) информационные ресурсы, средства информационного взаимодействия, информационная инфраструктура;
d) государство, владельцы, посредники .

5. Субъектами информационного пространства являются:
a) государство, юридические лица, физические лица;
b) пользователи, провайдеры, владельцы информации;
c) государство, пользователи, владельцы информации;
d) физические лица, юридические лица, посредники.

6. Принцип расширения субъектности информационного пространства заключается в:
a) увеличение объема передаваемой по Интернет информации;
b) увеличении количества интернет-провайдеров;
c) увеличении количества пользователей глобальной сети во всех странах;
d) это тенденция к вовлечению в современный информационный процесс новых субъектов, в том числе в виде негосударственных образований.
7. По данным Главного информационного центра МВД России, количество компьютерных преступлений ежегодно увеличивается в (раза):
a) 2;
b) 2,5;
c) 3,5;
d) 4.

8. По данным Главного информационного центра МВД России, средний ущерб, причиняемый потерпевшему от 1 компьютерного преступления, равен (млн руб.):
a) 0,5;
b) 1,7;
c) 2,5;
d) 3.

9. Компьютерные преступления – это те преступления, в которых:
a) с помощью несанкционированного доступа нарушается конфиденциальность информации;
b) результатом является нарушение системы безопасности предприятия;
c) объектом преступного посягательства является информация, обрабатываемая и хранящаяся в компьютерных системах, а орудием посягательства служит компьютер;
d) нарушается целостность и достоверность информации.

10. Конфиденциальность информации - это:
a) обеспечение доступа к информации тем лицам, у которых есть на это право;
b) обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;
c) обеспечение защиты той части информации в организации, которая является коммерческой тайной;
d) статус определенной части информации предприятия, который предоставляется для регламентации ее распространения.

11. Целостность информации - это:
a) свойство информации сохранять свою структуру и/или содержание в процессе передачи и хранения;

b) сохранение информации в е первоначальном виде;
c) передача информации и ее преобразование к исходному представлению;
d) отсутствие изменений в результате передачи информации по каналам связи.

12. Достоверность информации – это:
a) обязательное наличие у информации цифровой подписи ее собственника;
b) свойство информации, выражающееся в строгой принадлежности субъекту, который является ее источником, либо тому субъекту, от которого эта информация принята;
c) состояние защищенности информации, ее носителей, каналов передачи и среды ее распространения;
d) требование обеспечения информационной безопасности для средств хранения, использования, обработки и распространения информации.

13. Доступность информации – это:
a) состояние информации [ресурсов информационной системы], при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно;
b) предоставление возможности получения информации всем, кому она необходима;
c) предоставление владельцем информации всем пользователям, которым она необходима;
d) отсутствие ограничений на копирование и сохранение данных пользователями ИС.

14. Аутентификация субъекта – это:
a) получение субъектом идентификатора, предоставляющего право доступа к определенной части информации,;
b) это проверка подлинности субъекта с данным идентификатором;
c) ввод логина пользователем при входе в локальную сеть;
d) определение прав доступа субъекта с определенным логином и паролем.

15. Авторизация субъекта – это:
a) проверка подлинности его идентификатора;
b) это процедура предоставления законному субъекту, успешно прошедшему идентификацию и аутентификацию, соответствующих полномочий и доступных ресурсов системы (сети);
c) проверка соответствия субъекту своему идентификатору;
d) проверка его цифровой подписи.

16. Злоумышленник – это:
a) лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно;
b) лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.);
c) лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства;
d) нарушитель информационной безопасности, намеренно идущий на нарушение из корыстных побуждений..

17. Информационная безопасность– это:
    a) состояние защищенности информационных ресурсов, технологии их формирования и использования, поддерживающей инфраструктуры, а также прав субъектов информационной деятельности;
    b) деятельность по защите информации и данных с информационной системе предприятия;
    c) деятельность о обеспечению защиты информации от несанкционированного доступа в рамках информационной системы предприятия;
    d) состояние защищенности информационных ресурсов, технологии их формирования и использования, а также прав субъектов информационной деятельности.

18. Информационные процессы – это:
    a) преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
    b) процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
    c) совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
    d) получение субъектом возможности ознакомления с информацией, в том числе при помощи технических сред.

19. Собственник информации– это:
    a) физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;
    b) субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника, в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;
    c) участник правоотношений в информационных процессах;
    d) субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами.

20. Пользователь (потребитель) информации– это:
    a) физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;
    b) субъект, в полном объеме реализующий полномочия, пользования, распоряжения информацией в соответствии с законодательными актами;
    c) участник правоотношений в информационных процессах;
    d) субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации.

Раздел 2. Информационная безопасность ИС и сетей
Тема 2.6. Защита информации в компьютерных сетях. Защита на канальном и сеансовом уровне

Индивидуальное задание №10. Шифрование и электронно-цифровая подпись в системе документооборота. Программа PGP

1. Создайте личный ключ шифрования.

2. Запишите свои ключи pubring.pkr и sekring.skr на дискету для дальнейшего использования.
3. Запишите (export) свой публичный (открытый) ключ на дискету (или перешлите по сети) и передайте его участникам электронного обмена информацией.
4. Получите открытые ключи от участников обмена информацией и импортируйте их на свой компьютер.
5. Подпишите ключи партнёров и установите к ним режим доверия.
6. Создайте файл в MS Word, зашифруйте его, подпишите электронной подписью и передайте участнику обмена информацией, ключом которого шифровался файл.
7. Получите от участников обмена информацией зашифрованные и подписанные файлы и расшифруйте их.
8. Изучите разделы методических указаний и ответьте на вопросы для самопроверки, приведенные в конце темы.

Критерии оценивания компетенций (результатов) по уровням освоения учебного материала:

1 – репродуктивный (освоение знаний, выполнение деятельности по образцу, инструкции или под руководством), если самостоятельно (или с помощью преподавателя) выполненывсе пункты работы;

2 – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач; применение умений в новых условиях), если выполнены все пунктыработы самостоятельно и улучшена точность результата;

3 – творческий (самостоятельное проектирование экспериментальной деятельности; оценка и самооценка инновационной деятельности), если предложен более рациональный алгоритм решения задачи.

8.3.2. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и/или опыта деятельности

– оценивание проводится преподавателем в течении всего учебного процесса на основе выполнения текущих контрольных и индивидуальных заданий, самостоятельной работы за компьютером;

результаты выполнения практических работ предъявляются в виде отчетов оформленных в виде электронного файла;

– оценивание практических работ осуществляет преподаватель, который проводит практические занятия;

– экзамен принимает комиссия.

9. Методические указания для обучающихся по освоению дисциплины

Методические указания по дисциплине «Информационная безопасность» разработаны для всех 8-и практических работ курса. Вместе с индивидуальными заданиями по каждой практической работе и вопросами для самостоятельной работы они составляют методический комплект, доступный студентам в электронном виде.

Рекомендации, позволяющие обучающимся оптимальным образом организовать процесс изучения как теоретического учебного материала дисциплины, так и подготовки к практическим занятиям: изучение лекций, коллективное обсуждение тем на практических занятиях, индивидуальная работа за компьютером, самостоятельная работа над текущими темами, самостоятельная работа над индивидуальными заданиями.

По практической работе студент должен:

1. разобрать метод решения поставленной задачи и имеющиеся указания к её выполнению;
2. реализовать предложенный алгоритм на основе указанного ПО для решения задачи своего варианта задания на ПК;

3. выполнить необходимые операции на основе применения ПК для всех пунктов индивидуального задания;
4. сохранить результаты выполнения пунктов индивидуального задания в электронном виде;
5. представить результаты выполнения пунктов индивидуального задания в форме презентации, либо в л\другом электронном формате;
6. убедиться в достоверности полученных результатов;
7. отчитаться перед преподавателем по теоретической и практической части индивидуального задания.

10.Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Компьютерные классы, лекционные аудитории, оснащенные мультимедийным оборудованием.

11.Иные сведения и (или) материалы: (включаются на основании решения кафедры)

Оформление сведений о дополнении и изменении рабочей программы учебной дисциплины

Рабочие программы учебных дисциплин ежегодно обсуждаются, актуализируются на заседаниях ПМК, рассматриваются на заседаниях кафедр и утверждаются проректором по учебной работе, информация об изменениях отражается в листе сведений о дополнении и изменении рабочей программы учебной дисциплины. В случае существенных изменений программа полностью переоформляется. Обновленный электронный вариант программы размещается на сервере ГОУ ВПО «ДонАУиГС».

Изменения в РПУД могут вносится в следующих случаях:

– изменение государственных образовательных стандартов или других нормативных документов, в том числе локальных нормативных актов;

– изменение требований работодателей к выпускникам;

– разработка новых методик преподавания и контроля знаний студентов.

Ответственность за актуализацию РПУД несут преподаватели, реализующие дисциплину.

СВЕДЕНИЯ О ДОПОЛНЕНИИ И ИЗМЕНЕНИИ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ НА 20___/20___ УЧЕБНЫЙ ГОД

«Название дисциплины»

Направление подготовки

(профиль/магистерская программа)

ДОПОЛНЕНО (с указанием раздела РПУД)
ИЗМЕНЕНО (с указанием раздела РПУД)
УДАЛЕНО (с указанием раздела РПУД)

Реквизиты протокола заседания кафедры

от _____ № _____

дата