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
20.06.2017г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«Защита информации в корпоративных информационных системах»

Направление подготовки 09.04.03 «Прикладная информатика»

Донецк
2017

Рабочая программа учебной дисциплины «Защита информации в корпоративных информационных системах» для студентов 1 курса образовательного уровня «магистр» направления подготовки 09.04.03 «Прикладная информатика» очной формы обучения.

Автор,
разработчик: старший преподаватель, к.э.н., Н.Э.Тарусина

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

Заведующий кафедрой Н. В. Брадул

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

Цель освоения дисциплины – формирование компетенций магистров в области аудита состояния информационной безопасности корпоративных информационных систем.

Задачи учебной дисциплины:

– ознакомится с законодательным уровнем обеспечения информационной безопасности;

– изучить административный уровень информационной безопасности;

– научиться использовать передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации ИС.

Компетенции обучающегося, формируемые в результате освоения дисциплины:

Код соответствующей компетенции по ГОС	Наименование компетенций	Результат освоения (знать, уметь, владеть)
ОК-3	Готовность к саморазвитию, самореализации, использованию творческого потенциала	**Знать**: способы приобретения и использования в практической деятельности новых знаний и умений. **Уметь**: самостоятельно приобретать и использовать в практической деятельности новые знания и умения. **Владеть**: навыками самостоятельного осваивания новых версий пакетов прикладных программ и систем программирования.
ОПК-3	Способность исследовать современные проблемы и методы прикладной информатики и научно-технического развития ИКТ	**Знать:** историю становления и современные теоретические и практические концепции прикладной информатики. **Уметь:** с применением научных подходов осуществлять анализ проблем и методов прикладной информатики. **Владеть:** навыками проведения предпроектных исследований в сфере профессиональной деятельности.
ОПК-6	Способность к профессиональной эксплуатации современного электронного оборудования в соответствии с целями основной образовательной программы магистратуры	**Знать:** модели и структуры информационных сетей, информационные ресурсы сетей. **Уметь:** проводить диагностику неисправностей программных и аппаратных компонент информационных систем с использованием специального оборудования и инструментальных средств. **Владеть:** отдельными технологиями построения, отладки и сопровождения информационных систем и сетей.
ПК-9	Способность анализировать и оптимизировать	**Знать:** − особенности процессного подхода к управлению ИС;

	прикладные и информационные процессы	− методы анализа и оптимизации прикладных и информационных процессов. **Уметь:** − проводить реинжиниринг прикладных и информационных процессов; − выполнять критическое осмысление результатов реинжиниринга прикладных и информационных процессов; − применять метод анализа для изучения прикладных и информационных процессов. **Владеть:** − навыками реинжиниринга прикладных и информационных процессов и критического осмысление его результатов; − навыками логико-методологического анализа научного исследования и его результатов.
ПК-10	Способность проводить маркетинговый анализ ИКТ и вычислительного оборудования для рационального выбора инструментария автоматизации и информатизации прикладных задач	**Знать:** − основные методы, средства и стандарты информатики для решения прикладных задач, понимать их назначение и особенности; − возможности и области применения современных информационных систем предприятий и организаций; − основные способы маркетингового анализа. **Уметь:** − применять методы сравнительного анализа для оценки различных проектных решений; − определять последовательность действий, направленных на освоение новых технологий. **Владеть:** − основными практическими навыками работы с наиболее распространенными программно-техническими средствами для решения прикладных задач различных классов; − навыками оценки результатов проведения маркетингового анализа ИКТ и вычислительной техники.
ПК-21	Способность использовать передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации ИС	**Знать**: передовые методы оценки качества, информационной безопасности ИС. **Уметь**: использовать передовые методы оценки качества, надежности и информационной безопасности ИС. **Владеть**: передовыми методами оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации ИС.
ПК-28	Способность принимать участие в организации ИТ-инфраструктуры в	**Знать:** типовые программно-аппаратные средства и системы зашиты информации от несанкционированного доступа в

	управлении информационной безопасностью	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.

2. Место дисциплины в структуре основной образовательной программы

Дисциплина «Защита информации в корпоративных информационных системах» относится к обязательным дисциплинам вариативной части профессионального цикла учебного плана по направлению подготовки 09.04.03 «Прикладная информатика».

2.1. Требования к предварительной подготовке обучающегося

Дисциплина тесно связана с такими курсами, как: «Базы данных», «Информационная безопасность», «Корпоративные информационные системы», «Управление проектами информатизации предприятий».

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: «Внедрение корпоративных информационных систем на базе типовых проектных решений», «Администрирование баз данных».

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** (вносятся данные по реализуемым формам)	
		О	**З**	**Очная**	**Заочная**
				Семестр №2	**Семестр №**
Общая трудоемкость	**3**	**108**	**Х**	**Количество часов на вид работы:**	
Виды учебной работы, из них:					
Аудиторные занятия (всего)				**42**	**Х**
В том числе:					
Лекции				**28**	**Х**
Практические занятия				**14**	**Х**
Самостоятельная работа (всего)				**66**	**Х**
Промежуточная аттестация					
В том числе:					
экзамен				экзамен	**Х**

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. Проблемы безопасности корпоративной информации										
Тема 1.1. Основные понятия и анализ угроз информационной безопасности	2			8	10					
Тема 1.2. Политики безопасности	2	2		6	10					
Итого по разделу:	**4**	**2**		**14**	**20**					
Раздел 2. Технологии защиты корпоративных данных										
Тема 2.1. Криптографическая защита информации	6	2		6	14					
Тема 2.2. Идентификация, аутентификация и управление доступом	2	2		8	12					
Тема 2.3. Защита электронного документооборота	2			8	10					
Итого по разделу:	**10**	**4**		**22**	**36**					
Раздел 3. Комплексная защита корпоративных информационных систем										
Тема 3.1. Принципы комплексной защиты информации КИС	2	2		4	18					
Тема 3.2 Защита от вредоносных программ	2			6	8					
Тема 3.3 Обнаружение и предотвращение вторжений	2	2		4	8					
Тема 3.4 Межсетевое экранирование	2			6	8					
Тема 3.5 Виртуальные защищенные сети VPN	2	2		6	10					
Итого по разделу:	**10**	**6**		**16**	**52**					
Раздел 4. Управление информационной безопасностью										

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 4.1 Управление средствами обеспечения информационной безопасности	2			8	10					
Тема 4.2 Стандарты информационной безопасности	2	2		6	10					
Итого по разделу:	**4**	**2**		**14**	**20**					
Всего за семестр:	**28**	**14**		**66**	**108**					

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. Проблемы безопасности корпоративной информации				
Тема 1.1. Тема 1.2.	Формулируются основные понятия и определения информационной безопасности и анализируются угрозы информационной безопасности в корпоративных информационных системах; определяются базовые понятия политики безопасности и описываются основные виды политик и процедур безопасности в корпоративных информационных системах	**Практическое занятие №1**	**2**	
		1. Основные понятия и определения информационной безопасности	2	
		2. Базовые понятия политики безопасности; основные виды политик и процедур безопасности в корпоративных информационных системах		
Раздел 2. Технологии защиты корпоративных данных				
Тема 2.1. Тема 2.2. Тема 2.3.	Описываются такие криптографические методы защиты корпоративной информации, как симметричные	**Практическое занятие №2**	**2**	

Наименование раздела, темы дисциплины	Содержание разделов дисциплины	Содержание семинарских/практических занятий	Кол-во часов	
			о	з
1	2	3	4	5
	и асимметричные криптосистемы шифрования, комбинированные криптосистемы, электронная цифровая подпись, функции хэширования и управление криптоключами. Подробно описывается инфраструктура управления открытыми ключами PKI (Public Key Infrastructure). Рассматриваются идентификация, аутентификация и авторизация пользователя. Описываются методы аутентификации, использующие многоразовые и одноразовые пароли, методы строгой аутентификации и биометрической аутентификации пользователей, управление доступом по схеме однократного входа Single Sign-On. Рассматриваются методы и средства защиты электронного документооборота. Формулируется концепция и особенности защиты электронного документооборота. Анализируются методы и средства защиты баз данных. Подробно описывается защита электронного почтового документооборота.	1. Криптографическая защита информации	2	
		Практическое занятие №3	**2**	
		1. Идентификация, аутентификация и управление доступом	2	
Раздел 3. Комплексная защита корпоративных информационных систем				
Тема 3.1. Тема 3.2. Тема 3.3. Тема 3.4. Тема 3.5.	Рассматриваются принципы комплексной защиты информации в корпоративных информационных системах. Анализируются особенности архитектуры КИС и структура системы защиты информации в КИС. Формулируется стратегия комплексного обеспечения информационной безопасности и	**Практическое занятие №4**	**2**	
		1. Принципы комплексной защиты информации КИС	2	
		Практическое занятие №5	**2**	
		1. Обнаружение и предотвращение вторжений	2	
		Практическое занятие №6	**2**	

Наименование раздела, темы дисциплины	Содержание разделов дисциплины	Содержание семинарских/практических занятий	Кол-во часов	
			о	з
1	2	3	4	5
	описываются основные подсистемы информационной безопасности КИС. Описываются средства защиты от вредоносных программ. Приводится классификация вредоносных программ. Рассматриваются сигнатурный анализ и проактивные методы обнаружения вирусов и других вредоносных программ. Описывается защита корпоративной системы от вредоносных программ. Рассматриваются проблемы обнаружения и предотвращения вторжений; методы обнаружения и предотвращения вторжений в корпоративные информационные системы, а также защита от распределенных атак. Рассматриваются функции межсетевых экранов. Описываются схемы сетевой защиты на базе межсетевых экранов. Рассматривается применение персональных и распределенных сетевых экранов. Поясняется главное свойство сети VPN - туннелирование. Анализируются варианты построения виртуальных защищенных каналов. Рассматриваются варианты архитектуры сетей VPN и приводятся основные виды технической реализации VPN.	1. Виртуальные защищенные сети VPN	2	
Раздел 4. Управление информационной безопасностью				
Тема 4.1. Тема 4.2.	Рассматриваются методы управления средствами защиты корпоративной информации. Формулируются задачи управления системой информационной безопасности масштаба предприятия.	**Практическое занятие №7** 1. Стандарты информационной безопасности	**2** 2	

Наименование раздела, темы дисциплины	Содержание разделов дисциплины	Содержание семинарских/практических занятий		
			Кол-во часов	
			о	з
1	2	3	4	5
	Анализируются варианты архитектуры управления средствами безопасности. Особое внимание уделяется перспективной архитектуре централизованного управления безопасностью на базе глобальной и локальной политик безопасности. Приводится обзор современных систем управления информационной безопасностью. Описаны стандарты информационной безопасности. Рассматриваются основные международные стандарты информационной безопасности и, в частности, широко распространенный стандарт ISO 15408 «Общие критерии безопасности информационных технологий». Даются краткие описания популярных стандартов информационной безопасности для Интернета. Описываются отечественные стандарты безопасности информационных технологий.			

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).

Контрольные вопросы для самоподготовки

1. Сформулируйте понятие информационной безопасности ИС.
2. Объясните понятия целостности, конфиденциальности и доступности информации.
3. Объясните понятия идентификации, аутентификации и авторизации пользователя. Как они взаимосвязаны?
4. Укажите отличия санкционированного доступа от несанкционированного доступа к информации.
5. Сформулируйте определение политики безопасности.
6. Сформулируйте особенности избирательной и полномочной политики безопасности.

7. Объясните понятие «угроза безопасности ИС».
8. Укажите основные признаки классификации возможных угроз безопасности ИС.
9. Каковы основные виды угроз безопасности ИС по цели и степени воздействия?
10. Дайте краткую характеристику угроз безопасности, обозначаемых терминами: «троянский конь»,
«вирус», «червь»?
11. Перечислите и дайте краткую характеристику основных методов реализации угроз информационной безопасности.
12. Объясните суть комплексного подхода к обеспечению информационной безопасности ИС.
13. Объясните понятие «политика безопасности организации».
14. Какие разделы должна содержать документально оформленная политика безопасности?
15. Какие проблемы решает верхний уровень политики безопасности?
16. Какие задачи решает средний уровень политики безопасности?
17. Каковы особенности нижнего уровня политики безопасности?
18. Сформулируйте обязанности руководителей подразделений, администраторов и пользователей при реализации политики безопасности.
19. Опишите структуру политики безопасности организации.
20. Что представляют собой специализированные политики безопасности?
21. Приведите несколько примеров специализированных политик безопасности с описанием их особенностей.
22. Что представляют собой процедуры безопасности?
23. Приведите несколько примеров процедур безопасности с описанием их особенностей.
24. Сформулируйте основные этапы разработки политики безопасности организации.
25. Что такое криптография?
26. Дайте определения следующих понятий: криптограмма, криптоалгоритм, криптосистема.
27. В чем состоит коренное различие симметричных и асимметричных криптосистем?
28. Охарактеризуйте четыре основных режима работы блочного алгоритма.
29. Расскажите о способах комбинирования блочных алгоритмов для получения алгоритмов с более длинным ключом, сравните их между собой.
30. Каковы основные характеристики и режимы работы отечественного стандарта шифрования данных?
31. Сформулируйте концепцию криптосистемы с открытым ключом?
32. Дайте определение однонаправленной функции. Приведите примеры однонаправленных функций.
33. Каковы особенности однонаправленных функций с «потайным ходом»?
34. На чем основывается надежность криптоалгоритма шифрования RSA?
35. Опишите две основные процедуры, осуществляемые системой электронной цифровой подписи для подтверждения подлинности электронного документа.
36. Опишите отечественный стандарт цифровой подписи, укажите его преимущества по сравнению с алгоритмом цифровой подписи DSA.
37. Каково назначение хэш-функции и каким требованиям должна удовлетворять качественная хэш- функция?
38. Каким образом комбинированный метод шифрования позволяет сочетать достоинства асимметричных и симметричных криптосистем? Опишите протокол реализации комбинированного метода шифрования.
39. Опишите работу алгоритма Диффи - Хэллмана. Укажите достоинства этого алгоритма.
40. Каково назначение инфраструктуры открытых ключей PKI? Опишите функционирование инфраструктуры PKI.

41. Дайте определения понятий: идентификация, аутентификация, авторизация, администрирование. Что понимают под решением задач AAA?
42. Какие задачи решает подсистема управления идентификацией и доступом IAM (Identity and Access Management)?
43. На какие категории можно разделить процессы аутентификации в зависимости от сущностей, предъявляемых пользователем для подтверждения своей подлинности?
44. Перечислите основные атаки на протоколы аутентификации.
45. Опишите метод аутентификации на основе многоразовых паролей. Каковы недостатки этого метода?
46. Опишите метод аутентификации на основе одноразовых паролей. Каковы его достоинства и недостатки?
47. Сформулируйте принцип строгой аутентификации. Опишите типы процедур строгой аутентификации.
48. Объясните назначение PIN-кода и особенности его использования.
49. Объясните принцип работы двухфакторной аутентификации. Какие внешние носители информации используются для двухфакторной аутентификации пользователей? Каковы достоинства этого метода аутентификации?
50. Опишите функциональность и характеристики смарт-карт и USB-токенов.
51. Опишите методы биометрической аутентификации пользователя. Что означают коэффициент ошибочных отказов и коэффициент ошибочных подтверждений?
52. Поясните принцип управления доступом по схеме однократного входа с авторизацией Single Sign-On.
53. Укажите особенности построения и функционирования системы распределенного электронного документооборота.
54. Назовите угрозы информационной безопасности для СЭД и охарактеризуйте источники этих угроз.
55. Какие функции должны быть реализованы средствами защиты информации СЭД?
56. Сформулируйте основополагающие принципы построения современных КИС.
57. Охарактеризуйте четыре уровня управления КИС.
58. Укажите необходимые условия обеспечения санкционированного доступа к информационным ресурсам предприятия.
59. Какие важные системные функции может выполнять КИС при реализации в ней принципа централизованного управления?
60. Объясните значение управления рисками предприятия для создания системы эффективной защиты информации на этом предприятии.
61. Какие требования необходимо учитывать при разработке архитектуры КСЗИ?
62. Перечислите меры и средства защиты, применяемые при построении комплексной системы защиты информации КИС.
63. Укажите основные подсистемы информационной безопасности, входящие в состав КСЗИ.
64. Опишите особенности подсистемы защиты информации от несанкционированного доступа.
65. Опишите назначение и особенности подсистемы контроля эффективности защиты информации.
66. Опишите назначение и особенности подсистемы мониторинга и управления инцидентами ИБ.
67. Опишите назначение и особенности подсистемы обеспечения непрерывности функционирования средств защиты.
68. Что такое вредоносная программа? Охарактеризуйте основные типы вредоносных программ.

69. Укажите существенные отличия компьютерных вирусов от сетевых «червей». Опишите основные особенности «троянских» программ.
70. Опишите два основных подхода к обнаружению вредоносных программ.
71. Как выполняется сигнатурный анализ? Каковы его достоинства и недостатки?
72. Что представляют собой проактивные методы обнаружения?
73. Опишите принцип действия, достоинства и недостатки эвристических анализаторов.
74. Опишите принцип действия, достоинства и недостатки поведенческих блокираторов.
75. Назовите и опишите дополнительные модули антивирусных средств.
76. Каковы дополнительные меры и средства защиты от вредоносных программ, расширяющие возможности антивирусных программ?
77. Опишите меры и средства защиты от спама (нежелательной корреспонденции).
78. Каковы особенности реализации подсистемы защиты корпоративной информации от вредоносных программ и вирусов?
79. Сформулируйте понятия: обнаружение вторжений и предотвращение вторжений.
80. Укажите четыре признака системы IPS, отличающие ее от системы IDS.
81. Дайте определения понятий: сетевая система NIPS (network-based IPS) и хостовая система HIPS (host- based IPS).
82. Сформулируйте назначение и особенности применения специализированных средств - сканеров уязвимости (vulnerability assessment).
83. Какие методы анализа событий используются в процессе выявления вторжений?
84. В чем суть метода обнаружения аномального поведения?
85. В чем суть метода обнаружения злоупотреблений?
86. Опишите функциональность средств предотвращения вторжений системного (хостового) уровня
HIPS (Host-based IPS).
87. Опишите функциональность средств предотвращения вторжений сетевого уровня NIPS (network- based IPS).
88. Сформулируйте подход к защите от распределенных атак типа «отказ в обслуживании» DDoS (Distributed Denial of Service).
89. Какими свойствами и функциями должна обладать современная IPS для успешного обнаружения и предотвращения вторжений?
90. Опишите структуру и функционирование подсистемы предотвращения вторжений в КИС.
91. Что такое виртуальные защищенные сети VPN (Virtual Private Network)?
92. Сформулируйте концепцию построения виртуальных защищенных сетей VPN.
93. Объясните понятия «виртуальный защищенный туннель», «туннелирование» и «инкапсуляция».
94. Дайте развернутые определения таких устройств VPN, как VPN-клиент, VPN-сервер и VPN-шлюз безопасности.
95. Поясните особенности структуры и функционирования двух основных схем виртуальных защищенных каналов.
96. Каковы функции инициатора туннеля и терминатора туннеля?
97. Какие методы используют для обеспечения безопасности сетей VPN?
98. Опишите классификацию сетей VPN по рабочему уровню модели взаимодействия открытых систем
OSI (Open Systems Interconnection).
99. Каковы основные варианты архитектуры сетей VPN? Дайте пояснение для каждого из трех основных вариантов.
100. Укажите основные виды технической реализации VPN и дайте пояснения для каждого из них.
101. Какие российские компании выпускают VPN-продукты в настоящее время?

102. Опишите возможности и основные характеристики семейства VPN-продуктов CSP VPN 3.0
103. российской компании «С-Терра СиЭсПи».
104. Назовите задачи системы управления информационной безопасностью КИС.
105. Как осуществляется управление учетными записями и правами доступа к рабочим станциям, серверам и другим активным устройствам КИС?
106. В чем суть концепции глобального управления безопасностью GSM (Global Security Management)?
107. Объясните понятия «глобальная и локальная политики безопасности».
108. Опишите функционирование системы управления информационной безопасностью GSM.
109. Как осуществляется защита ресурсов в системе управления информационной безопасностью GSM?
110. Как осуществляется управление средствами информационной безопасности масштаба предприятия в системе GSM?
111. Опишите централизованное управление безопасностью, реализованное в продуктах Застава.
112. Опишите возможности системы управления Cisco Security Manager и программно-аппаратного комплекса управления Cisco MARS.
113. Какие функции реализуют продукты IBM Tivoli для обеспечения информационной безопасности КИС?
114. Назовите основные продукты IBM Tivoli и опишите их возможности.
115. Какие задачи решает система управления безопасностью IBM Proventia Management SiteProtector?
116. Сформулируйте главную задачу стандартов информационной безопасности с позиций производителей и потребителей продуктов информационных технологий, а также специалистов по сертификации этих продуктов.
117. Назовите основные международные стандарты информационной безопасности.
118. Дайте краткую характеристику международного стандарта ISO/IEC 17799:2000 (BS 7799-1:2000).
119. Каковы основные особенности германского стандарта BSI «Руководство по защите информационных технологий для базового уровня защищенности»?
120. Опишите содержание и укажите значение международного стандарта ISO 15408 «Общие критерии безопасности информационных технологий.
121. Перечислите стандарты для беспроводных сетей и дайте их краткую характеристику.
122. Назовите стандарты информационной безопасности для Интернета.
123. Каковы назначение и особенности функционирования протокола SET (Security Electronics Transaction)?
124. Каковы назначение и функциональность протоколов SSL (Secure Socket Layer) и IPSec? В чем эти протоколы существенно различаются?
125. Каковы назначение и функциональность инфраструктуры управления открытыми ключами PKI?
126. Перечислите российские стандарты безопасности информационных технологий.
127. Каково назначение стандарта ГОСТ Р ИСО/МЭК 15408? Назовите и охарактеризуйте три основные части этого стандарта.

5.2. Перечень основной учебной литературы

1. Гатчин Ю. А. Теория информационной безопасности и методология защиты информации: учебное пособие [Электронный ресурс] / Ю.А. Гатчин, В.В. Сухостат. – СПб.: СПбГУ ИТМО, 2010. – 98 с. – Режим доступа: http://window.edu.ru/resource/984/71984/files/itmo477.pdf

2. 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

3. 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

5.3. Перечень дополнительной литературы

1. Нестеров С. А. Информационная безопасность и защита информации: учебное пособие [Электронный ресурс] / С. А. Нестеров. – СПб.: Изд-во Политехн. ун-та, 2009. – 126 с. – Режим доступа:
http://window.edu.ru/catalog/pdf2txt/462/67462/48880.

2. Макаренко С. И. Информационная безопасность: учебное пособие для студентов вузов [Электронный ресурс] / С. И. Макаренко. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 371 с. – Режим доступа: http://window.edu.ru/catalog/pdf2txt/775/77775/58783

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

1. Горбачевская Е.Н. Исследование механизмов защиты данных в корпоративных информационных системах [Электронный ресурс]. – Режим доступа: http://cyberleninka.ru/article/n/issledovanie-mehanizmov-zaschity-dannyh-v-korporativnyh-informatsionnyh-sistemah

2. Зашита информации в корпоративных сетях ИС управления [Электронный ресурс]. – Режим доступа: http://bizbook.online/business_menedjment/zashita-informatsii-korporativnyih-setyah.html

3. Аверченков В.И. Служба защиты информации: организация и управление: учеб. пособие для вузов [Электронный ресурс] / В.И. Аверченков, М.Ю. Рытов. – Брянск: БГТУ, 2005. – 186 с. – Режим доступа: http://nouscbryansk.ru/core/wp-content/themes/natural-health/document/method_posoby/%D1%81%D0%BB%D1%83%D0%B6%D0%B1%D0%B0%20%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D1%8B%20%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8.%20%D1%83%D1%87%D0%B5%D0%B1%D0%BD%D0%BE%D0%B5%20%D0%BF%D0%BE%D1%81%D0%BE%D0%B1%D0%B8%D0%B5.pdf

4. Войтик А.И. Экономика информационной безопасности: Учебное пособие вузов [Электронный ресурс] / А.И. Войтик, В.Г. Прожерин. – СПб.: НИУ ИТМО, 2012. – 120 с. – Режим доступа: http://window.edu.ru/resource/853/78853/files/itmo923.pdf

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 проведении лекций используется аудитория с мультимедийным оборудованием. Аудиторные занятии проводятся в компьютерных классах с доступом к сети Интернет. Для проведения консультаций в online-режиме используется LMS Moodle и Skype.

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 (ответы на вопросы, тестовые задания), включая задания для самостоятельной работы.

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.

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 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)

Темы рефератов

1. Основные понятия и анализ угроз информационной безопасности.
2. Политики безопасности.
3. Криптографическая защита информации.
4. Идентификация, аутентификация и управление доступом.
5. Защита электронного документооборота.
6. Принципы комплексной защиты информации КИС.
7. Защита от вредоносных программ.
8. Обнаружение и предотвращение вторжений.
9. Межсетевое экранирование.
10. Виртуальные защищенные сети VPN.
11. Управление средствами обеспечения информационной безопасности.
12. Стандарты информационной безопасности.

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

Методические материалы, определяющие процедуры оценивания, могут включать в себя следующие основные элементы:

– Оценивание проводится преподавателем в течении всего учебного процесса на основе выполнения текущих индивидуальных практических заданий; а также на экзамене.

– Результаты выполнения практических работ предъявляются в виде отчетов оформленных текстовом редакторе;

– Оценивание практических работ осуществляет преподаватель, который проводит практические занятия.

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.

9. Методические рекомендации (указания) для обучающихся по освоению дисциплины

С целью обеспечения эффективного усвоения студентами материала курса при выполнении ими индивидуальных работ необходимо, чтобы эти работы выполнялись студентами после проработки соответствующего материала и усвоения порядка проведения экспериментальной части работы. Рекомендуется использование компьютеров при выполнении исследований в индивидуальной работе. Основная рекомендация сводится к обеспечению равномерной активной работы студентов над курсом в течение семестра: они должны прорабатывать курс прослушанных лекций, готовиться к выполнению индивидуальных работ. При выполнении заданий, вынесенных на самостоятельное изучение, необходимо наряду с библиотечным фондом пользоваться различными базами знаний, размещенными в сети Интернет.

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