Автономная некоммерческая организация высшего образования

«СЕВЕРО-ЗАПАДНЫЙ ОТКРЫТЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

«Утверждаю»
Проректор по УМР
О.М. Вальц
«07» сентября 2017 г.

Рабочая программа дисциплины

«Информационная безопасность и защита информации»

Направление подготовки: **27.04.03 «Системный анализ и управление»**

Направленность(профиль): **«Системный анализ организационно-управленческой деятельности в больших системах»**

Квалификация: **магистр**

Форма обучения: **заочная**

Санкт-Петербург
2017

Рабочая программа дисциплины «Информационная безопасность и защита информации» разработана в соответствии с требованиями ФГОС ВО по направлению 27.04.03 «Системный анализ и управление».

Основным документом для разработки рабочей программы является рабочий учебный план направления 27.04.03 «Системный анализ и управление» и магистерской программы подготовки «Системный анализ организационно-управленческой деятельности в больших системах».

Учебные и методические материалы по учебной дисциплине размещены в электронной информационно-образовательной среде университета.

Разработчик: к.т.н., доцент Л.В. Боброва, заведующая кафедрой информационных технологий и безопасности

Смирнова Н.А., зам. генерального директора ПО «Ленстройматериалы», кандидат технических наук, доцент

Рабочая программа рассмотрена на заседании кафедры информационных технологий и безопасности «06» сентября 2017 года, протокол № 1.

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Информационная безопасность и защита информации» изучается магистрантами по направлению 27.04.03 Системный анализ и управление в одном семестре.

Дисциплина включает в себя разделы: принципы обеспечения защиты информации, уровни информационной защиты; системы безопасности и их дефекты, криптографические системы обеспечения защиты информации; атаки системы; основные направления работ по созданию систем комплексной защиты информационной системы объекта; мобильные программы.

1.1.Основной целью изучения дисциплины является систематизация и расширение знаний и навыков по защите информации в рамках современной концепции обеспечения информационной безопасности различных объектов.

1.2.Основными задачами изучения дисциплины является:

-Знание базовых понятий защиты информации
-Основных аспектов комплексной информационной безопасности
-Технических средств защиты информации
-Обеспечения безопасности сетевых коммуникаций
-Основ криптографии и криптоанализа, основных методов
-Законов и нормативных актов обеспечения информационной безопасности.

1.3.В результате освоения дисциплины у студента должны быть сформированы следующие общекультурные, общепрофессиональные и профессиональные компетенции:

общекультурные

готовность действовать в нестандартных ситуациях, нести социальную и этическую ответственность за принятые решения (ОК-2);

общепрофессиональные

способность разработать практические рекомендации по использованию качественных и количественных результатов научных исследований (ОПК-4);

профессиональные

Способностью формировать технические задания и участвовать в разработке аппаратных и (или) программных средств, экспертно-аналитических систем поддержки принятия оптимальных решений (ПК-4);

1.4. Квалификационные требования к уровню освоения содержания дисциплины

Дисциплина базируется на знаниях, полученных при изучении дисциплин: «Системные методы обработки данных», «Программное обеспечение компьютерных сетей и информационных систем», «Компьютерные технологии в науке» по направлению 27.04.03 Системный анализ или управление подготовки

магистра техники и технологии.

Знания, умения и навыки, полученные при изучении настоящего предмета, используются при написании квалификационной работы магистра.

В результате изучения дисциплины студент должен:

Знать:

- содержание и общие принципы обеспечения информационной безопасности на законодательном уровне;

- основные меры и подходы к обеспечению информационной безопасности на административном уровне;

- содержание и способы процедурного уровня защиты информации;

- методы и средства реализации программно-технического уровня защиты информационных систем;

- достоинства и недостатки, а также возможности применения изучаемых уровней информационной защиты.

Уметь:

- проводить обследование объекта (предприятия) на предмет выявления реальных угроз несанкционированного доступа к конфиденциальной информации;

- разрабатывать политику безопасности и мероприятия по обеспечению информационной безопасности системы управления предприятием в соответствии с требованиями по защищенности технических и программных средств от утечки конфиденциальной информации;

- внедрять систему информационной безопасности в действующую структуру предприятия;

Владеть:

- основами защиты информационных систем от несанкционированного доступа.

Быть компетентным в проблемных вопросах теории системных исследований и перспективах развития математических методов системного анализа и теории принятия решений.

2.МЕСТО ДИСЦИПЛИНЫ В УЧЕБНОМ ПРОЦЕССЕ

Дисциплина базируется на знаниях, полученных при изучении дисциплин: «Системные методы обработки данных», «Программное обеспечение компьютерных сетей и информационных систем», «Компьютерные технологии в науке» по направлению 27.04.03 Системный анализ и управление подготовки магистра техники и технологии.

Знания, умения и навыки, полученные при изучении настоящего предмета, используются при написании квалификационной работы магистра.

3. ОБЪЕМ ДИСЦИПЛИНЫ В ЗАЧЕТНЫХ ЕДИНИЦАХ

№ п/п	Наименование модулей и номера тем учебной дисциплины	Трудоёмкость по учебному плану (час/з е)	Виды занятий					
			Лекции	Практические занятия	Лабораторные занятия	Самостоятельная работа	Контрольная работа	Зачёт (экзамен)
1	2	3	4	5	6	7	8	9
1	Введение	4				4		
	Раздел 1. Принципы обеспечения защиты информации. Уровни информационной	16	0,5			15,5		
	Понятие безопасности	8	0,25			7,75		
	Системы безопасности и их дефекты	8	0,25			7,75		
	Раздел 2. Криптографические системы и	16	0,5	1		14,5		
	Основы криптографии	4	0,5			3,5		
	Шифрование с секретным ключом	3		0,5		2,5		
	Шифрование с открытым ключом	3		0,5		2,5		
	Аутентификация пользователей	5	0,25			4,75		
	Защиты паролей в системе UNIX	5	0,25	0,5		4,25		
	Совершенствование безопасности паролей	6		0,5		5,5		
	Раздел 4. Атаки системы снаружи и	16	0,5	1		14,5		
	Атаки системы снаружи	5	0,25	0,25		4,5		
	Атаки изнутри системы	5	0,25	0,25		4,5		
	Атака системы безопасности	6		0,5		5,5		
	Раздел 5. Основные направления работ по	16	1	1		14		

№ п/п	Наименование модулей и номера тем учебной дисциплины	Трудоёмкость по учебному плану (час/з е)	Виды занятий					
			Лекции	Практические занятия	Лабораторные занятия	Самостоятельная работа	Контрольная работа	Зачёт (экзамен)
	Механизмы защиты	5	0,25	0,25		4,5		
	Перечни возможностей	5	0,25	0,25		4,5		
	Надежные системы	6		0,5		5,5		
	Раздел 6. Мобильные программы	16	1	1		14		
	Метод «Песочниц»	4	0,25	0,25		3,5		
	Интерпретация	4	0,25	0,25		3,5		
	Программы с подписями	4	0,25	0,25		3,5		
	Безопасность в система Java	4	0,25	0,25		3,5		
	Заключение	4				4		
	Итого	**108/3**	**4**	**6**		**98**	**1**	**диф. зач.**

4.СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Введение

Основные понятия защиты информации. Роль и место конфиденциальной информации в обеспечении безопасности Российской Федерации. Общие принципы обеспечения информационной безопасности объекта (предприятия). Структура дисциплины.

РАЗДЕЛ 1. Принципы обеспечения защиты информации. Уровни информационной защиты

Классификация и источники наиболее распространенных угроз информационной безопасности. Анализ уязвимости информационных систем. Классификация сетевых атак. Безопасность локальных вычислительных сетей и интегрированных информационных систем управления. Распределенное хранение файлов. Оценка рисков. Требования по обеспечению информационной безопасности информационной системы. Уровни информационной защиты.

Знаменитые дефекты системы безопасности UNIX, TENEX, 0S/360. Принципы проектирования систем безопасности.

РАЗДЕЛ 2. Криптографические системы и криптоанализ

Криптология. Криптосистемы. Понятие стойкости криптографического алгоритма. Анализ надежности криптосистем. Классические методы криптоанализа. Архитектура систем защиты данных.

РАЗДЕЛ 3. Технические аспекты обеспечения защиты информации

Методы реализации программно-технического уровня защиты информационных систем. Программно-аппаратные средства комплексной защиты информации. Подсистема идентификации и аутентификации. Подсистема управления доступом. Подсистема протоколирования аудита. Конфиденциальность и целостность данных и сообщений. Контроль участников взаимодействия. регистрация и наблюдения. Излечения элементов ПЭВМ. Экранирование помещений, предназначенных для размещения ПЭВМ и технических средств обработки информации.

РАЗДЕЛ 4. Атаки системы снаружи и изнутри

Основные характеристики технических средств защиты от несанкционированного доступа. Требования по защите информации от несанкционированного доступа для автоматизированных систем защиты третьей, второй и первой групп. Требования по защите информации от несанкционированного доступа для средств вычислительной техники. Требования к межсетевым экранам.

РАЗДЕЛ 5. Основные направления работ по созданию систем комплексной защиты информационной системы объекта (предприятия)

Организация работ по защите от несанкционированного доступа интегрированной информационной системы управления предприятием. Классификация интегрированных информационных систем управления предприятием. Система компьютерной безопасности. Оснащение объекта техническими средствами противодействия экономическому шпионажу и защиты речевой информации. Этапы проведения работ по обеспечению информационной безопасности предприятия.

РАЗДЕЛ 6. Мобильные программы

Мобильные программы, апплеты. Примеры. Метод «песочницы». Интерпретируемые программы. Программы с подписями. Примеры систем безопасности. Безопасность в системе Java.

Заключение

Международные документы, регламентирующие деятельность по обеспечению защиты информации. Политика информационной безопасности Российской Федерации. Законы РФ в области информационной безопасности. Документы ФАПСИ.

Проблемные вопросы. Перспективы развития. Исследования в области безопасности. Рекомендации по дальнейшему овладению дисциплиной «Информационная безопасность и защита информации».

5. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

5.1.ПЕРЕЧЕНЬ ТЕМ КУРСОВЫХ РАБОТ

Не предусмотрены учебным планом.

5.2.ПЕРЕЧЕНЬ ТЕМ КОНТРОЛЬНОЙ РАБОТЫ

1 Угрозы информационной безопасности предприятия (организации) и способы борьбы с ними

2 Современные средства защиты информации

3 Современные системы компьютерной безопасности

4 Современные средства противодействия экономическому шпионажу

5 Современные криптографические системы

6 Криптоанализ, современное состояние

7 Правовые основы защиты информации

8 Технические аспекты обеспечения защиты информации. Современное состояние

9 Атаки на систему безопасности и современные методы защиты

10 Современные пути решения проблемы информационной безопасности РФ

5.3.ВОПРОСЫ ДЛЯ ПОДГОТОВКИ К ДИФЕРЕНЦИРОВАННОМУ ЗАЧЕТУ

1. Что такое информационная безопасность?
2. Какие предпосылки и цели обеспечения информационной безопасности?
3. В чем заключаются национальные интересы РФ в информационной сфере?
4. Что включает в себя информационная борьба?
5. Какие пути решения проблем информационной безопасности РФ существуют?
6. Каковы общие принципы обеспечения защиты информации?
7. Какие имеются виды угроз информационной безопасности предприятия (организации)?
8. Какие источники наиболее распространенных угроз информационной безопасности существуют?
9. Какие виды сетевых атак имеются?
10. Какими способами снизить угрозу сниффинга пакетов?
11. Какие меры по устранению угрозы IP-спуфинга существуют?
12. Что включает борьба с атаками на уровне приложений?
13. Какие существуют проблемы обеспечения безопасности локальных вычислительных сетей?
14. В чем заключается распределенное хранение файлов?
15. Что включают в себя требования по обеспечению комплексной системы информационной безопасности?

16. Какие уровни информационной защиты существуют, их основные составляющие?
17. В чем заключаются задачи криптографии?
18. Зачем нужны ключи?
19. Какая схема шифрования называется многоалфавитной подстановкой?
20. Какие системы шифрования вы знаете?
21. Что включает в себя защита информации от несанкционированного доступа?
22. В чем заключаются достоинства и недостатки программно-аппаратных средств защиты информации?
23. Какие виды механизмов защиты могут быть реализованы для обеспечения идентификации и аутентификации пользователей?
24. Какие задачи выполняет подсистема управления доступом?
25. Какие требования предъявляются к подсистеме протоколирования аудита?
26. Какие виды механизмов защиты могут быть реализованы для обеспечения конфиденциальности данных и сообщений?
27. В чем заключается контроль участников взаимодействия?
28. Какие функции выполняет служба регистрации и наблюдения?
29. Что такое информационно-опасные сигналы, их основные параметры?
30. Какие требования необходимо выполнять при экранировании помещений, предназначенных для размещения вычислительной техники?
31. Какой процесс называется аутентификацией пользователя?
32. Какие схемы аутентификации вы знаете?
33. Что такое смарт-карты?
34. Какие требования предъявляются к современным криптографическим системам защиты информации?
35. Что такое симметричная криптосистема?
36. Какие виды симметричных криптосистем существуют?
37. Что такое асимметричная криптосистема?
38. Что понимается под односторонней функцией?
39. Как классифицируются криптографические алгоритмы по стойкости?
40. В чем заключается анализ надежности криптосистем?
41. Что такое дифференциальный криптоанализ?
42. В чем сущность криптоанализа со связанными ключами?
43. В чем сущность линейного криптоанализа?
44. Какие атаки изнутри вы знаете?
45. Какая программа называется логической бомбой?
46. Какими способами можно проверить систему безопасности?
47. Что является основными характеристиками технических средств защиты информации?
48. Какие требования предъявляются к автоматизированным системам защиты третьей группы?

49. Какие требования предъявляются к автоматизированным системам защиты второй группы?
50. Какие требования предъявляются к автоматизированным системам защиты первой группы?
51. Какие классы защиты информации от несанкционированного доступа для средств вычислительной техники имеются? От чего зависит выбор класса защищенности?
52. Какие требования предъявляются к межсетевым экранам?
53. Какие имеются показатели защищенности межсетевых экранов?
54. Какие атаки системы снаружи вы знаете?
55. Какая программа называется вирусом?
56. Какая атака называется атакой отказа в обслуживании?
57. Какие виды вирусов вы знаете?
58. Какие вирусы называются паразитическими?
59. Как распространяются вирусы?
60. Какие методы обнаружения вирусов вы знаете?
61. Какая программа называется монитором обращения?
62. Что представляет собой домен?
63. Как осуществляется защита при помощи ACL-списков?
64. Какой список называется перечнем возможностей?
65. Какие способы защиты перечней возможностей вы знаете?
66. Из чего состоит высоконадежная вычислительная база (TCB)?
67. Какие модели многоуровневой защиты вы знаете?
68. В чем заключается организация работ по защите от несанкционированного доступа интегрированной информационной системы управления предприятием?
69. Какие характеристики положены в основу системы классификации информационных систем управления предприятием?
70. Какие задачи решает система компьютерной безопасности?
71. Какие пути защиты информации в локальной сети существуют?
72. Какие задачи решают технические средства противодействия экономическому шпионажу?
73. Какой порядок организации системы видеонаблюдения?
74. Что включает в себя защита информационных систем с помощью планирования?
75. Какие условия работы оцениваются при планировании?
76. Из каких этапов состоят работы по обеспечению информационной безопасности предприятия?
77. Что такое мобильные программы?
78. Что такое концепция потоков?
79. Что представляет собой метод «Песочниц»?
80. Что такое интерпретация?
81. Что такое программы с подписями?
82. Что представляет собой безопасность в системе Java?
83. Назовите несколько примеров политик безопасности пакета JDK 1.2?

84. Какие международные документы регламентируют деятельность по обеспечению защиты информации?

85. Что понимают под политикой информационной безопасности?

86. Что включает в себя политика информационной безопасности РФ?

87. Какие нормативные документы РФ определяют концепцию защиты информации?

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине по решению кафедры оформлен отдельным приложением к рабочей программе.

7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Основная литература

1 Башлы П. Н. Информационная безопасность [Электронный учебник] : Учебное пособие / Башлы П. Н., 2012, Евразийский открытый институт. - 311 c. Режим доступа: http://iprbookshop.ru/10677

2 Спицын В. Г. Информационная безопасность вычислительной техники [Электронный учебник] : Учебное пособие / Спицын В. Г., 2011, Эль Контент, Томский государственный университет систем управления и радиоэлектроники. - 148 c.

Режим доступа: http: //iprbookshop .ru/13936

Дополнительная литература

1 Афанасьев М. П. Информационная безопасность и защита информации : учеб.-метод. комплекс, информ. ресурсы дисциплины, учеб. пособие / М. П. Афанасьев, 2010, Изд-во СЗТУ. - 134 с.

2 Информационная безопасность и защита информации : учеб.-метод. комплекс / сост.: М. П. Афанасьев, О. В. Афанасьева, 2009, Изд-во СЗТУ. - 121 с.

8. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО – ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ "ИНТЕРНЕТ", НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.Электронная информационно-образовательная среда АНО ВО "СЗТУ" (ЭИОС СЗТУ) [Электронный ресурс]. - Режим доступа: http://edu.nwotu.ru/

2.Электронная библиотека АНО ВО "СЗТУ" [Электронный ресурс]. - Режим доступа: http://lib.nwotu.ru:8087/jirbis2/

3.Электронно-библиотечная система IPRbooks [Электронный ресурс]. - Режим доступа: http://www.iprbookshop.ru/

4.Информационная система "Единое окно доступа к образовательным ресурсам" [Электронный ресурс]. - Режим доступа: http://window.edu.ru/

5.Информационная системы доступа к электронным каталогам библиотек сферы образования и науки (ИС ЭКБСОН)[Электронный ресурс]. - Режим доступа: http://www.vlibrary.ru/

Программное обеспечение

1. ППП MS Office 2016
2. Текстовый редактор Блокнот
   Браузеры IE, Google Chrome, Mozilla Firefox.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, практические занятия, контрольную работу, самостоятельную работу студента, консультации.

9.1. При изучении тем из модулей 1-6 студентам необходимо повторить лекционный учебный материал, изучить рекомендованную литературу, а также учебный материал, находящийся в указанных информационных ресурсах.

На завершающем этапе изучения каждого модуля необходимо, воспользовавшись предложенными вопросами для самоконтроля, размещенными в электронной информационной образовательной среде (ЭИОС), проверить качество усвоения учебного материала

В случае затруднения в ответах на поставленные вопросы рекомендуется повторить учебный материал.

9.2. После изучения каждого модуля дисциплины необходимо ответить на вопросы контрольного теста по данному модулю с целью оценивания знаний и получения баллов.

9.3. По завершению изучения учебной дисциплины в семестре студент обязан пройти промежуточную аттестацию. Вид промежуточной аттестации определяется рабочим учебным планом. Форма проведения промежуточной аттестации – компьютерное тестирование с использованием автоматизированной системы тестирования знаний студентов в ЭИОС.

9.4. К промежуточной аттестации допускаются студенты, выполнившие требования рабочего учебного плана.

9.5. Особенности освоения дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

Обучение обучающихся с ограниченными возможностями здоровья при

необходимости, по личному заявлению, осуществляется на основе адаптированной рабочей программы с использованием специальных методов обучения и дидактических материалов, составленных с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся (обучающегося).

10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

При осуществлении образовательного процесса по дисциплине используются следующие информационные технологии:

1. Internet – технологии:

WWW (англ. World Wide Web – Всемирная Паутина) – технология работы в сети с гипертекстами;

FTP (англ. File Transfer Protocol – протокол передачи файлов) – технология передачи по сети файлов произвольного формата;

IRC (англ. Internet Relay Chat – поочередный разговор в сети, чат) – технология ведения переговоров в реальном масштабе времени, дающая возможность разговаривать с другими людьми по сети в режиме прямого диалога;

ICQ (англ. I seek you – я ищу тебя, можно записать тремя указанными буквами) – технология ведения переговоров один на один в синхронном режиме.

2. Дистанционное обучение с использованием ЭИОС на платформе Moodle.

3. Технология мультимедиа в режиме диалога.

4. Технология неконтактного информационного взаимодействия (виртуальные кабинеты, лаборатории).

5. Гипертекстовая технология (электронные учебники, справочники, словари, энциклопедии) и т.д.

11.ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

1. Библиотека.
2. Справочно-правовая система Консультант Плюс.
3. Электронная информационно-образовательная среда университета.
4. Локальная сеть с выходом в Интернет.

12. БАЛЛЬНО-РЕЙТИНГОВАЯ СИСТЕМА

Виды учебной работы	**баллы**
Участие в online занятиях, прослушивание видео лекций	0 - 5
Контрольный тест к разделу 1 - 2	0 - 15
Контрольный тест к разделу 3 - 4	0 - 15
Контрольный тест к разделу 5 - 6	0 - 15
Контрольная работа	0 - 20
Итоговый контрольный тест	0 - 30
ИТОГО	0-100

Бонусы	баллы
- за активность	0 - 10
- за участие в ОЛИМПИАДЕ (в зависимости от занятого места)	0 - 50
- за участие в НИРС (в зависимости от работы)	0 - 50
- за оформление заявок на полезные модели (рац. предложения)	0 - 50

Балльная шкала оценки

Итоговая оценка (дифференцированный зачет)	Баллы
«неудовлетворительно»	менее 51
«удовлетворительно»	51 – 68
«хорошо»	68 – 85
«отлично»	86 – 100

Оценка по контрольной работе

Оценка	Количество баллов
отлично	18 - 20
хорошо	15 - 17
удовлетворительно	12 - 14
неудовлетворительно	менее 12

Приложение
к рабочей программе дисциплины
«Информационная безопасность и защита информации»
для направления подготовки
27.04.03 Системный анализ и управление

ФОНД

ОЦЕНОЧНЫХ СРЕДСТВ

1. Перечень формируемых компетенций

Код компетенции	Наименование и (или) описание компетенции
ОК-2	Готовность действовать в нестандартных ситуациях, нести социальную и этическую ответственность за принятые решения
ОПК-4	Способностью разработать практические рекомендации по использованию качественных и количественных результатов научных исследований
ПК-4	Способностью формировать технические задания и участвовать в разработке аппаратных и (или) программных средств, экспертно-аналитических систем поддержки принятия оптимальных решений

2. Паспорт фонда оценочных средств

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1	Раздел 1.	ОК-2, ОПК-4, ПК-4	Контрольный тест 1
2	Раздел 2	ОК-2, ОПК-4, ПК-4	Практическая работа Контрольный тест 2
3	Раздел 3.	ОК-2, ОПК-4, ПК-4	Практическая работа Контрольный тест 3
4	Раздел 4	ОК-2, ОПК-4, ПК-4	Практическая работа Контрольный тест 4
5	Раздел 5	ОК-2, ОПК-4, ПК-4	Практическая работа Контрольный тест 5
6	Раздел 6	ОК-2, ОПК-4, ПК-4	Практическая работа Контрольный тест 6
7	Разделы 1 - 6	ОК-2, ОПК-4, ПК-4	Контрольная работа Итоговый контрольный тест

3. Показатели и критерии оценивания компетенций по этапам формирования

Этапы освоения компетенции	Показатели достижения заданного уровня освоения компетенций	Критерии оценивания результатов обучения			
		2	3	4	5
Первый этап	Знать: (ОК-2; ОПК-4; ПК-4) -содержание и общие принципы обеспечения информационной безопасности на законодательном уровне; -основные меры и подходы к обеспечению информационной безопасности на административном уровне; -содержание и способы процедурного уровня защиты информации; методы и средства реализации программно-технического уровня защиты информационных систем; -достоинства и недостатки, а также возможности применения изучаемых уровней информационной защиты.	Демонстрирует частичные знания без грубых ошибок	Знает достаточно в базовом объеме	Знает достаточно в базовом объеме	Демонстрирует высокий уровень знаний
Второй этап	Уметь: (ОК-2; ОПК-4; ПК-4) -проводить обследование объекта (предприятия) на предмет выявления реальных угроз несанкционированного доступа к конфиденциальной информации; -разрабатывать политику безопасности и мероприятия по обеспечению информационной безопасности системы управления предприятием в соответствии с требованиями по защищенности технических и программных средств от утечки конфиденциальной информации; -внедрять систему информационной безопасности в действующую структуру предприятия;	Демонстрирует частичные умения, допуская грубые ошибки	Демонстрирует частичные умения без грубых ошибок	Умеет применять знания в базовом (стандартном) объеме	Демонстрирует высокий уровень умений
Третий этап	Владеть (ОК-2; ОПК-4; ПК-4) -основами защиты информационных систем от несанкционированного доступа.	Демонстрирует низкий уровень владения, допуская грубые ошибки	Демонстрирует частичные владения без грубых ошибок	Владеет базовыми приемами	Демонстрирует владения на высоком уровне

4. Шкалы оценивания

(балльно-рейтинговая система)

Виды учебной работы	баллы
Участие в online занятиях, прослушивание видео лекций	0 - 5
Контрольный тест к разделу 1 - 2	0 - 15
Контрольный тест к разделу 3 - 4	0 - 15
Контрольный тест к разделу 5 - 6	0 - 15
Контрольная работа	0 - 20
Итоговый контрольный тест	0 - 30
ИТОГО	0-100

Балльная шкала оценки

Итоговая оценка (дифференцированный зачет)	Баллы
«неудовлетворительно»	менее 51
«удовлетворительно»	51 – 68
«хорошо»	68 – 85
«отлично»	86 – 100

5.Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций при изучении учебной дисциплины в процессе освоения образовательной программы

5.1.Типовой вариант задания на контрольную работу

1 Угрозы информационной безопасности предприятия (организации) и способы борьбы с ними
2 Современные средства защиты информации
3 Современные системы компьютерной безопасности
4 Современные средства противодействия экономическому шпионажу
5 Современные криптографические системы
6 Криптоанализ, современное состояние
7 Правовые основы защиты информации
8 Технические аспекты обеспечения защиты информации. Современное состояние
9 Атаки на систему безопасности и современные методы защиты
10 Современные пути решения проблемы информационной безопасности РФ

5.2.Типовой тест промежуточной аттестации

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

10) Принципом информационной безопасности является принцип недопущения:
- Неоправданных ограничений при работе в сети (системе)
- Рисков безопасности сети, системы
- Презумпции секретности

6.Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

6.1.Итоговый контрольный тест доступен студенту только во время тестирования, согласно расписания занятий или в установленное деканатом время.

6.2.Студент информируется о результатах текущей успеваемости.

6.3.Студент получает информацию о текущей успеваемости, начислении бонусных баллов и допуске к процедуре итогового тестирования от преподавателя или в ЭИОС.

6.4.Производится идентификация личности студента.

6.5.Студентам, допущенным к промежуточной аттестации, открывается итоговый контрольный тест.

6.6.Тест закрывается студентом лично по завершении тестирования или автоматически по истечении времени тестирования.