МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета _____ С.М. Пасмурнов

«31» августа 2017 г.

РАБОЧАЯ ПРОГРАММА

дисциплины

«Компьютерные преступления в распределённых компьютерных системах»

Специальность 10.05.01 КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

Специализация Безопасность распределённых компьютерных систем

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2016

Автор программы _____ /Остапенко Г.А./

Заведующий кафедрой Систем информационной безопасности _____ / Остапенко А.Г./

Руководитель ОПОП _____ / Остапенко А.Г./

Воронеж 2017

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цель дисциплины обеспечить усвоение будущими инженерам, специализирующимся в области организации и технологии защиты информации, поведенческих мотивов, целей, условий и механизмов совершения компьютерных преступлений, а также законодательных основ их предотвращении

1.2. Задачи освоения дисциплины

- привить навыки формирования требований по защите информации в различных КС;
- ознакомить с требованиями к защите автоматизированных информационных систем (ИС) от несанкционированного доступа (НСД) на территории Российской Федерации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Компьютерные преступления в распределённых компьютерных системах» относится к дисциплинам вариативной части блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Компьютерные преступления в распределённых компьютерных системах» направлен на формирование следующих компетенций:

ПСК-3.3 способностью использовать современные среды и технологии, разработки программного обеспечения в распределенных компьютерных системах с учетом требований информационной безопасности ;

ПСК-3.4 способностью организовывать защиту информации в распределенных компьютерных системах

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ПСК-3.3	знать - основные принципы построения защищенных РКС и построения систем обнаружения компьютерных атак; - основные категории требований к программной и программно-аппаратной реализации средств защиты информации
	уметь - обосновывать требования к программной и аппаратной реализации средств защиты;
	владеть - навыками выявления и устранения уязвимостей компьютерной сети;

ПСК-3.4	знать - особенности защиты информации на узлах компьютерной сети и концепцию защиты информации в государственных и коммерческих структурах; - основные модели информационной безопасности и системные вопросы защиты программ и данных; - основные категории требований к программной и программно-аппаратной реализации средств защиты информации;
	уметь - анализировать защищенность систем, определять объекты защиты информации в КС и сетях;
	владеть - навыками проведения анализа рисков и администрирования безопасности распределенных компьютерных систем.

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Компьютерные преступления в распределённых компьютерных системах» составляет 11 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры		
		8	9	10
Аудиторные занятия (всего)	198	36	54	108
В том числе:				
Лекции	126	18	36	72
Практические занятия (ПЗ)	72	18	18	36
Самостоятельная работа	162	72	36	54
Курсовой проект	+			+
Часы на контроль	36	-	-	36
Виды промежуточной аттестации - экзамен, зачет	+	+	+	+
Общая трудоемкость: академические часы зач.ед.	 396 11	 108 3	 90 2.5	 198 5.5

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Прак зан.	СРС	Всего, час
1	Общие понятия и характеристика компьютерных преступлений (КП)	Понятие и разновидность компьютерных преступлений. Характеристика компьютерных преступлений Обзор угроз политике безопасности компьютерных систем. Перечень моделей	22	12	26	60
2	Законодательная база борьбы с КП	Раскрытие и расследование компьютерных преступлений. Законодательная основа борьбы с компьютерными преступлениями	22	12	26	60
3	Анализ вредоносного ПО	Детальный анализ вредоносного программного обеспечения. Классификация вирусов. Эвристический анализ. Анализ разрушающих воздействий программного обеспечения.	22	12	26	60
4	Сетевые атаки и системы обнаружения вторжений	Компьютерные сетевые атаки. Системы обнаружения вторжения и межсетевого экранирования. Анализ разрушающих воздействий. Методы обнаружения и борьбы. Удаленные компьютерные сетевые атаки: распределенные подходы организации.	20	12	28	60
5	Политики безопасности КС	Политики безопасности компьютерных систем. Организация сетевой политики безопасности.	20	12	28	60
6	Компьютерные преступления и их моделирование	Характеристика основных видов преступлений с использованием банковских пластиковых карт. Математическая модель распространения вредоносного программного обеспечения в социальных информационных системах. Компьютерные преступления на социальные информационные сети. Предупреждение компьютерных преступлений.	20	12	28	60
		Итого	**126**	**72**	**162**	**360**

5.2 Перечень лабораторных работ

Не предусмотрено учебным планом

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины предусмат-

ривает выполнение курсовых проектов в 10 семестрах для очной формы обучения.

Примерная тематика курсового проекта:

1. Исследование защищенности MD5.
2. Особенности работы WPA2: анализ уязвимостей.
3. Защищенная работа с JavaScript.
4. Построение защищенных CMS для веб-сайтов.
5. Технология защищенного кода: Основные подходы в работе с отладчиками.
6. Особенности анализа сетевого трафика: работы с протоколами.
7. Анализ уязвимостей PHP.
8. Анализ уязвимостей CGI.
9. Подходы к организации защиты SQL.
10. Анализ систем обнаружения и предотвращения вторжений.
11. Проведение анализа подсистемы безопасности в ОС Linux.
12. Проведение анализа уязвимостей в web-технологиях.
13. Анализ безопасности облачных технологий.
14. Анализ защищенности Windows Server.
15. Особенности работы с OllyDbg: безопасный кодинг.

Курсовой проект включат в себя графическую часть и расчетно-пояснительную записку.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе:

«аттестован»;

«не аттестован».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ПСК-3.3	знать - основные принципы построения защищенных РКС и построения систем обнаружения компьютерных атак; - основные категории требований к программной и програм-	знание основных принципов построения защищенных РКС и построения систем обнаружения компьютерных атак; - основные категории требований к программной и программно-аппаратной реа-	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	мно-аппаратной реализации средств защиты информации	лизации средств защиты информации		
	уметь - обосновывать требования к программной и аппаратной реализации средств защиты;	умение обосновывать требования к программной и аппаратной реализации средств защиты;	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть - навыками выявления и устранения уязвимостей компьютерной сети;	владение навыками выявления и устранения уязвимостей компьютерной сети;	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПСК-3.4	знать - особенности защиты информации на узлах компьютерной сети и концепцию защиты информации в государственных и коммерческих структурах; - основные модели информационной безопасности и системные вопросы защиты программ и данных; - основные категории требований к программной и программно-аппаратной реализации средств защиты информации;	знание особенностей защиты информации на узлах компьютерной сети и концепцию защиты информации в государственных и коммерческих структурах; - основные модели информационной безопасности и системные вопросы защиты программ и данных; - основные категории требований к программной и программно-аппаратной реализации средств защиты информации;	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь - анализировать защищенность систем, определять объекты защиты информации в КС и сетях;	умение анализировать защищенность систем, определять объекты защиты информации в КС и сетях;	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть - навыками проведения анализа рисков и администрирования безопасности распределенных компьютерных систем.	владение навыками проведения анализа рисков и администрирования безопасности распределенных компьютерных систем.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 8, 9, 10 семестре для очной формы обучения по двух/четырехбалльной системе:

«зачтено»

«не зачтено»

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Зачтено	Не зачтено
ПСК-3.3	знать - основные принципы построения защищенных РКС и построения систем обнаружения компьютерных атак; - основные категории требований к программной и программно-аппаратной реализации средств защиты информации	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь - обосновывать требования к программной и аппаратной реализации средств защиты;	Решение стандартных практических задач	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	владеть - навыками выявления и устранения уязвимостей компьютерной сети;	Решение прикладных задач в конкретной предметной области	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ПСК-3.4	знать - особенности защиты информации на узлах компьютерной сети и концепцию защиты информации в государственных и коммерческих структурах; - основные модели информационной безопасности и системные вопросы защиты программ и данных; - основные категории требований к программной и программно-аппаратной реализации средств защиты информации;	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь - анализировать защищенность систем, определять объекты защиты информации в КС и сетях;	Решение стандартных практических задач	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	владеть - навыками проведения анализа рисков и администрирования безопасности распределенных компьютерных систем.	Решение прикладных задач в конкретной предметной области	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

или «отлично»; «хорошо»; «удовлетворительно»; «неудовлетворительно».

Компетенция	**Результаты обучения, характеризующие сформированность компетенции**	**Критерии оценивания**	**Отлично**	**Хорошо**	**Удовл.**	**Неудовл.**
ПСК-3.3	знать - основные принципы построения защищенных РКС и построения систем обнаружения компьютерных атак; - основные категории требований к программной и программно-аппаратной реализации средств защиты информации	Тест	Выполнение теста на 90- 100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь - обосновывать требования к программной и аппаратной реализации средств защиты;	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	владеть - навыками выявления и устранения уязвимостей компьютерной сети;	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ПСК-3.4	знать - особенности защиты информации на узлах компьютерной сети и концепцию защиты информации в государственных и коммерческих структурах; - основные модели информационной безопасности и системные вопросы защиты программ и данных; - основные категории требований к программной и программно-аппаратной реализации средств защиты информации;	Тест	Выполнение теста на 90- 100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов

	уметь - анализировать защищенность систем, определять объекты защиты информации в КС и сетях;	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	владеть - навыками проведения анализа рисков и администрирования безопасности распределенных компьютерных систем.	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

7.2.1 Примерный перечень заданий для подготовки к тестированию

1.Основные виды «компьютерных преступлений».

2.Как определяется состав компьютерных преступлений.

3.Обобщенная классификация компьютерных преступлений в Российской Федерации. Основные подходы к классификации.

4.Положения уголовного кодекса РФ в отношении компьютерных преступлений. Ответственность за совершение компьютерных преступлений различного характера.

5.Принцип действия международного кодификатора компьютерных преступлений.

6.Принцип организации системы обеспечения оперативно-розыскных мероприятий.

7.Характерные отличия в зарубежном законодательстве в области компьютерных преступлений.

8.Общие понятия при построении политики безопасности системы.

9.Дискретные модели безопасности.

10.Модели на основе анализа угроз системе.

11.Модели конечных состояний.

12.Признаки по которым можно классифицировать вирусы.

13.Классификация вирусов по среде обитания.

14.Основные виды вредоносного программного обеспечения.

15.Загрузочные вирусы. Принцип работы.

16.Файловые вирусы. Перезаписывающие, паразитические, вирусы без точки входа, компаньон-вирусы.

17.Вирусы семейства Macro.

18.Полиморфик вирусы. Уровни полиморфизма.

19.Стелс-вирусы: загрузочные, файловые, макро.

20.Резидентные вирусы. Характеристики резидентных вирусов.

21.Утилиты скрытого администрирования.

22.Троянский конь. Логическая бомба. Полиморфные генераторы. Сетевые вирусы.

23.Методы обнаружения и удаления компьютерных вирусов. Типы антивирусов. Основные подходы в организации построения антивирусного программного обеспечения.

24.Сканеры, CRC-сканеры, Блокировщики, Иммунизаторы.

25.Ложное срабатывание при поиске вирусов. Сканирование по запросу. Сканирование на лету.

26.Принцип обнаружения неизвестного вируса.

27.Профилактика вирусного заражения компьютера. Основные правила защиты.

28.Восстановление пораженных вирусами объектов. Основные сложности.

29.Основные виды «компьютерных преступлений».

30.Как определяется состав компьютерных преступлений.

31.Обобщенная классификация компьютерных преступлений в Российской Федерации. Основные подходы к классификации.

32.Положения уголовного кодекса РФ в отношении компьютерных преступлений. Ответственность за совершение компьютерных преступлений различного характера.

33.Принцип действия международного кодификатора компьютерных преступлений.

34. Принцип организации системы обеспечения оперативно-розыскных мероприятий.

35. Характерные отличия в зарубежном законодательстве в области компьютерных преступлений.

36. Общие понятия при построении политики безопасности системы.

37. Дискретные модели безопасности.

38. Модели на основе анализа угроз системе.

39. Модели конечных состояний.

40. Признаки по которым можно классифицировать вирусы.

41. Классификация вирусов по среде обитания.

42. Основные виды вредоносного программного обеспечения.

43. Загрузочные вирусы. Принцип работы.

44. Файловые вирусы. Перезаписывающие, паразитические, вирусы без точки входа, компаньон-вирусы.

45. Вирусы семейства Macro.

46. Полиморфик вирусы. Уровни полиморфизма.

47. Стелс-вирусы: загрузочные, файловые, макро.

48. Резидентные вирусы. Характеристики резидентных вирусов.

49. Утилиты скрытого администрирования.

50. Троянский конь. Логическая бомба. Полиморфные генераторы. Сетевые вирусы.

51. Методы обнаружения и удаления компьютерных вирусов. Типы антивирусов. Основные подходы в организации построения антивирусного программного обеспечения.

52. Сканеры, CRC-сканеры, Блокировщики, Иммунизаторы.

53. Ложное срабатывание при поиске вирусов. Сканирование по запросу. Сканирование на лету.

54. Принцип обнаружения неизвестного вируса.

55. Профилактика вирусного заражения компьютера. Основные правила защиты.

56. Восстановление пораженных вирусами объектов. Основные сложности.

57. Компоненты сетевой атаки. Принцип организации.

58. Классификация сетевых атак по составу.

59. Модели традиционных сетевых атак.

60. Классификация сетевых атак по применению. Коммутируемая инфраструктура. Анти-снифферы.

61. IP-spoofing. Противодействие спуфингу.

62. Атаки типа отказа в обслуживании. Противодействие им.

63. Атаки типа Main-in-the-Middle.

64. Атаки на уровне приложений. Противодействие им.

65. Принцип организации сетевой разведки. Злоупотребление доверием. Переадресация портов.

66. Уровни модели ISO/OSI.

67. Классификация удаленных атак на распределенные вычислительные системы.

68. Анализ сетевого трафика. Способы реализации.

69. Подмена доверенного объекта или субъекта распределенной сети.

70. Внедрение в распределенную сеть ложного объекта путем навязывания ложного маршрута.

71. Атака типа «Ложный ARP-сервер». Сценарий реализации.

72. Реализация атаки типа ложный DNS-сервер.

73. Навязывание хосту ложного маршрута с использованием протокола ICMP с целью создания ложного маршрутизатора.

74. Принцип подмены одного из субъектов TCP-соединения в сети Internet.

75. Принцип построения IDS-систем (отличия от IDPS-систем). ри основных подхода к обнаружению атак.

76. Основные недостатки систем обнаружения сетевых вторжений.

77. Типы организации систем обнаружения вторжения: хостовая и сетевая IDS.

78. Атаки на IDS: fragmentation Reassembly Timeoutattacks, TTL Basedattacks, OverlappingFragments.

79. Сигнатурные и поведенческие IDS. Основные характеристики. От-

личия в работе.

80. Распределѐнные системы обнаружения вторжений. Системы предотвращения вторжений. Определение новых методов сетевых вторжений.

81. Варианты реакций на обнаруженную атаку с помощью IDS. Выявление злоупотреблений. Эвристический анализ.

82. Состав и структура аппаратной реализации системы обнаружения вторжений.

83. Характерные особенности преступлений, совершаемых с использованием банковских карт.

84. Классификация банковских пластиковых карт.

85. Уязвимости механизма функционирования банковских карт в привязке к процессинговому центру, банкам эмитента и эквайрера.

86. Личность компьютерного преступника. Два подхода к определению личности преступника.

87. Типовые следственные действия при раскрытии компьютерных преступлений

7.2.2 Примерный перечень заданий для решения стандартных задач

1.Согласно закону HIPAA требования безопасности включают общие положения и детальные требования в следующих специфических областях:

технические меры безопасности +

экономические требования

организационные требования +

2. Какие основные функции определяет политика?

безопасность внутри организации +

место каждого служащего в системе безопасности +

характер поведения сотрудников вне организации

безопасность взаимодействия между организациями

3. Какие разделы политики являются общепринятыми?

введение

цель +

ответственность +

заключение

4. Что такое аудит безопасности?

отслеживание определенного типа событий во всех системах +

предотвращение взлома всех систем

защита всех систем от несанкционированного доступа

разграничение доступа ко всем системам

5. Какие требования по отношению к паролям указываются в политике безопасности?

минимальное количество символов в пароле +

средняя длина пароля

требования к наличию символов из различных групп +

6. Какие стандартные события учитываются при аудите безопасности?

попытки входа в систему успешные +

создание файлов
изменение файлов
попытки удаленного доступа неудачные +
выключение +
7. Цели процедуры обработки инцидентов (IRP):
защита систем организации +
восстановление операций +
прекращение деятельности организации на время угрозы
снижения уровня антирекламы +
снижение количества внешних связей на время угрозы
8. Какие типы событий должны быть указаны в DRP?
события, связанные с отдельными системами или устройствами +
события, связанные с отдельными компьютерами
события, связанные с хранилищами данных +
события, связанные с организацией в целом +
события, связанные с взаимодействием организаций

7.2.3 Примерный перечень заданий для решения прикладных задач

1.Дайте определение компьютерного преступления согласно закона 1030 США.

компьютерное преступление – это преднамеренный несанкционированный доступ в компьютер +

компьютерное преступление – это неумышленный несанкционированный доступ в компьютер

компьютерное преступление – это неумышленный санкционированный доступ в компьютер

2.Что входит в величину ущерба, нанесенного при совершении компьютерного преступления?

исправление повреждений от взлома +
стоимость определения величины ущерба +
ущерб от взлома конфиденциальных данных

3.Что не входит в величину ущерба, нанесенного при совершении компьютерного преступления?

ущерб от взлома конфиденциальных данных +
стоимость проведения расследования
затраты на модернизацию системы безопасности +

4. Какая атака на компьютерную систему с целью мошенничества с кредитными картами считается преступлением?

сумма ущерба превышает 1000 долл. и злоумышленник завладел 20 номерами кредитных карт +

сумма ущерба превышает 1000 долл. и злоумышленник завладел 10 номерами кредитных карт

сумма ущерба не превышает 1000 долл. и злоумышленник завладел 20 номерами кредитных карт +

5. Какая атака на компьютерную систему с целью мошенничества с кредитными картами считается преступлением?

сумма ущерба превышает 1000 долл. и злоумышленник завладел 10 номерами кредитных карт

сумма ущерба не превышает 5000 долл. и злоумышленник завладел 10 номерами кредитных карт

сумма ущерба превышает 5000 долл. и злоумышленник завладел 15 номерами кредитных карт+

6. Сбор какой информации без соответствующей санкции является преступлением (согласно закона 1030 США)?

заголовки электронной почты

содержимое письма электронной почты +

содержимое вложенных файлов +

7. Сбор какой информации без соответствующей санкции является преступлением (согласно закона 1030 США)?

номера портов TCP и UDP отправителя и получателя

содержимое письма +

IP-адреса отправителя и получателя

вложенные файлы в письмо +

8. Сбор какой информации без соответствующей санкции является преступлением (согласно закона 1030 США)?

тема письма электронной почты +

содержимое вложенных файлов +

номера портов TCP и UDP отправителя и получателя

9. К каким организациям применяются правила закона HIPAA?

общественным организациям

правоохранительным органам

организациям планирования здравоохранения +

10. К каким организациям применяются правила закона HIPAA?

информационным центрам здравоохранения +

общественным организациям

организациям планирования здравоохранения +

7.2.4 Примерный перечень вопросов для подготовки к зачету

1.Понятие «компьютерные преступления». Два основных подхода.

2.Криминалистическое толкование компьютерных преступлений.

3.Состав компьютерных преступлений.

4.Классификация компьютерных преступлений в Российской Федерации.

5.Законодательная база в области компьютерных преступлений России. Ответственность за совершение компьютерных преступлений различного характера.

6.Международный кодификатор компьютерных преступлений.

7.Незаконные воздействия на компьютерную информацию.

8.Система обеспечения оперативно-розыскных мероприятий.

9.Зарубежное законодательство в области компьютерных преступлений.

10.Политика безопасности. Жизненный цикл компьютерной системы. Угрозы компьютерной системе.

11.Канал утечки. Виды каналов утечки. Канал воздействия. Описание моделей безопасности с использованием субъектов и объектов.

12.Дискретные модели безопасности. Модель Адепт. Пространство Хартстона. Матрица доступа.

13.Модель управления доступом.

14.Модели на основе анализа угроз системе. Игровая модель. Модель системы безопасности с полным перекрытием.

15.Модели конечных состояний. Модель уровней секретности. Модель Белла-Лападула. Модель китайской стены. Модель Low-Water-Mark (Биба).

16.Признаки по которым можно классифицировать вирусы.

17.Классификация вирусов по среде обитания.

18.Классы вредоносного программного обеспечения.

19.Загрузочные вирусы. Принцип работы. Встраивание в MBR и BR.

20.Файловые вирусы. Перезаписывающие, паразитические, вирусы без точки входа, компаньон-вирусы, файловые черви, Link-вирусы, OBJ-, LIB-вирусы и вирусы в исходных текстах.

21.Вирусы семейства Macro. Характерные примеры проявлениями вирусов семейства macro.

22.Полиморфик вирусы. Уровни полиморфизма.

23.Стелс-вирусы: загрузочные, файловые, макро.

24.Резидентные вирусы. Характеристики резидентных вирусов.

25.Утилиты скрытого администрирования. Троянский конь. Логическая бомба. Полиморфные генераторы. Сетевые вирусы.

26.Методы обнаружения и удаления компьютерных вирусов. Типы антивирусов.

27.Сканеры, CRC-сканеры, Блокировщики, Иммунизаторы. Ложное срабатывание. Сканирование по запросу. Сканирование на лету.

28.Обнаружение неизвестного вируса. Проникновение в таблицу векторов прерываний. Встраивание в DOS. Другие способы проникновения.

29.Обнаружение загрузочного вируса. Обнаружение макро-вируса.

30.Профилактика вирусного заражения компьютера. Основные правила защиты.

31.Восстановление пораженных вирусами объектов.

32.Уязвимость. Угроза. Атака. Компоненты сетевой атаки.

33.Классификация сетевых атак по составу.

34.Модели традиционных атак.

35.Классификация сетевых атак по применению. Коммутируемая инфраструктура. Анти-снифферы.

36.IP-spoofing. Противодействие спуфингу. Отказ в обслуживании. Противодействие.

37.Атаки типа Main-in-the-Middle.

38.Атаки на уровне приложений. Противодействие.

39.Сетевая разведка. Злоупотребление доверием. Переадресация пор-

тов.

40.Классификация удаленных атак на распределенные вычислительные системы.

41.Анализ сетевого трафика. Способы реализации.

42.Подмена доверенного объекта или субъекта распределенной сети.

43.Внедрение в распределенную сеть ложного объекта путем навязывания ложного маршрута.

44.Навязывание хосту ложного маршрута с использованием протокола ICMP с целью создания ложного маршрутизатора.

45.Принцип подмены одного из субъектов TCP-соединения в сети Internet.

46.IDS-системы. Три основных подхода к обнаружению атак.

47.Недостатки современных систем обнаружения.

48.Сигнатурные и поведенческие IDS.

49.Состав и структура аппаратной реализации системы обнаружения вторжений.

50.Преступления, совершаемые с использованием банковских карт.

51.Классификация банковских карт.

52.Уязвимости механизма функционирования банковских карт в привязке к процессинговому центру, банкам эмитента и эквайрера.

53.Личность компьютерного преступника. Два подхода к определению личности преступника.

54.Раскрытие и расследование компьютерных преступлений.

55.Типовые следственные ситуации первоначального этапа и следственные действия в области раскрытия компьютерных преступлений.

7.2.5 Примерный перечень заданий для решения прикладных задач

1.Понятие «компьютерные преступления». Два основных подхода.

2.Криминалистическое толкование компьютерных преступлений.

3.Состав компьютерных преступлений.

4.Классификация компьютерных преступлений в Российской Федерации.

5.Законодательная база в области компьютерных преступлений России. Ответственность за совершение компьютерных преступлений различного характера.

6.Международный кодификатор компьютерных преступлений.

7.Незаконные воздействия на компьютерную информацию.

8.Система обеспечения оперативно-розыскных мероприятий.

9.Зарубежное законодательство в области компьютерных преступлений.

10.Политика безопасности. Жизненный цикл компьютерной системы. Угрозы компьютерной системе.

11.Канал утечки. Виды каналов утечки.

12.Описание моделей безопасности с использованием субъектов и объектов.

13.Дискретные модели безопасности.

14.Модель Адепт.
15.Пространство Хартстона.
16.Матрица доступа.
17.Модель Харрисона, Руззо и Ульмана.
18.Модель Take Grant.
19.Модель управления доступом.
20.Модели на основе анализа угроз системе.
21.Игровая модель.
22.Модель системы безопасности с полным перекрытием.
23.Модели конечных состояний.
24.Модель уровней секретности.
25.Модель Белла-Лападула.
26.Модель китайской стены.
27.Модель Low-Water-Mark (Биба).
28.Модель Лендвера.
29.Модель Кларка-Вилсона.
30.Модель Липнера.
31.Признаки по которым можно классифицировать вирусы.
32.Классификация вирусов по среде обитания.
33.Классы вредоносного программного обеспечения.
34.Загрузочные вирусы. Принцип работы.
35.Технологии встраивания вируса в MBR и BR.
36.Файловые вирусы.
37.Перезаписывающие, паразитические, вирусы без точки входа.
38.Компаньон-вирусы, файловые черви, Link-вирусы.
39.OBJ-, LIB-вирусы и вирусы в исходных текстах.
40.Вирусы семейства Macro. Характерные примеры проявлениями вирусов семейства macro.
41.Полиморфик вирусы. Уровни полиморфизма.
42.Стелс-вирусы: загрузочные, файловые, макро.
43.Резидентные вирусы. Характеристики резидентных вирусов.
44.Утилиты скрытого администрирования.
45.Троянский конь. Логическая бомба.
46.Полиморфные генераторы. Сетевые вирусы.
47.Методы обнаружения и удаления компьютерных вирусов.
48.Типы антивирусов.
49.Сканеры, CRC-сканеры, Блокировщики, Иммунизаторы.
50.Ложное срабатывание. Сканирование по запросу. Сканирование на лету.
51.Обнаружение неизвестного вируса. Проникновение в таблицу векторов прерываний. Встраивание в DOS. Другие способы проникновения.
52.Обнаружение загрузочного вируса.
53.Обнаружение макро-вируса.
54.Профилактика вирусного заражения компьютера. Основные правила защиты.

55.Восстановление пораженных вирусами объектов.

56.Уязвимость. Угроза. Атака. Компоненты сетевой атаки.

57.Классификация сетевых атак по составу.

58.Модели традиционных атак.

59.Классификация сетевых атак по применению. Коммутируемая инфраструктура. Анти-снифферы.

60.IP-spoofing. Противодействие спуфингу. Отказ в обслуживании. Противодействие.

61.Атаки типа Main-in-the-Middle.

62.Атаки на уровне приложений. Противодействие.

63.Сетевая разведка. Злоупотребление доверием.

64.Переадресация портов при сетевом взаимодействии.

65.Уровни модели ISO/OSI.

66.Классификация удаленных атак на распределенные вычислительные системы.

67.Анализ сетевого трафика.

68.Способы атаки типа анализ сетевого трафика.

69.Подмена доверенного объекта или субъекта распределенной сети.

70.Внедрение в распределенную сеть ложного объекта путем навязывания ложного маршрута.

71.Атака типа «Ложный ARP-сервер». Сценарий реализации.

72.Реализация атаки типа ложный DNS-сервер. Сценарий 1: злоумышленник в одном сегменте сети с DNS-сервером, но в разных сегментах с атакуемым объектом. Сценарий 2: злоумышленник в одном сегменте сети с атакуемым хостом, но в разных сегментах с DNS-сервером. Шторм DNS-запросов.

73.Навязывание хосту ложного маршрута с использованием протокола ICMP с целью создания ложного маршрутизатора.

74.Принцип подмены одного из субъектов TCP-соединения в сети Internet.

75.IDS-системы.

76.Три основных подхода к обнаружению атак с помощью IDS-систем.

77.Недостатки современных систем обнаружения.

78.Хостовая и сетевая IDS. Характеристики.

79.Атаки на IDS (Fragmentation Reassembly Timeoutattacks, TTL Basedattacks, OverlappingFragments).

80.Сигнатурные и поведенческие IDS.

81.Распределѐнные системы обнаружения вторжений.

82.Системы предотвращения вторжений.

83.Определение новых методов сетевых вторжений.

84.Варианты реакций на обнаруженную атаку с помощью IDS.

85.Выявление злоупотреблений при анализе сетевых атак. Эвристический анализ.

86.Состав и структура аппаратной реализации системы обнаружения вторжений.

87.Преступления, совершаемые с использованием банковских карт.

88.Классификация банковских карт.

89.Уязвимости механизма функционирования банковских карт в привязке к процессинговому центру, банкам эмитента и эквайрера.

90.Анализ состояний информационной безопасности в работе процессингового центра.

91.Личность компьютерного преступника.

92.Два подхода к определению личности преступника.

93.Раскрытие и расследование компьютерных преступлений.

94.Типовые следственные ситуации первоначального этапа и следственные действия в области раскрытия компьютерных преступлений.

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

(Например: Экзамен проводится по тест-билетам, каждый из которых содержит 10 вопросов и задачу. Каждый правильный ответ на вопрос в тесте оценивается 1 баллом, задача оценивается в 10 баллов (5 баллов верное решение и 5 баллов за верный ответ). Максимальное количество набранных баллов – 20.

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 6 баллов.

2. Оценка «Удовлетворительно» ставится в случае, если студент набрал от 6 до 10 баллов

3. Оценка «Хорошо» ставится в случае, если студент набрал от 11 до 15 баллов.

4. Оценка «Отлично» ставится, если студент набрал от 16 до 20 баллов).

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Общие понятия и характеристика компьютерных преступлений (КП)	ПСК-3.3; ПСК-3.4	Тест, контрольная работа, защита практических работ, требования к курсовому проекту
2	Законодательная база борьбы с КП	ПСК-3.3; ПСК-3.4	Тест, контрольная работа, защита практических работ, требования к курсовому проекту
3	Анализ вредоносного ПО	ПСК-3.3; ПСК-3.4	Тест, контрольная работа, защита практических работ, требования к курсовому проекту
4	Сетевые атаки и системы обнаружения вторжений	ПСК-3.3; ПСК-3.4	Тест, контрольная работа, защита практических работ, требования к курсовому проекту

5	Политики безопасности КС	ПСК-3.3; ПСК-3.4	Тест, контрольная работа, защита практических работ, требования к курсовому проекту
6	Компьютерные преступления и их моделирование	ПСК-3.3; ПСК-3.4	Тест, контрольная работа, защита практических работ, требования к курсовому проекту

7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методики выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Защита курсовой работы, курсового проекта или отчета по всем видам практик осуществляется согласно требованиям, предъявляемым к работе, описанным в методических материалах. Примерное время защиты на одного студента составляет 20 мин.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

Основная

1. Методическое обеспечение оценки и регулирования рисков распределенных информационных систем: Учеб. пособие / Г. А. Остапенко [и др.]. - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2011. - 178 с. - 182-77; 250 экз.

2. Остапенко А.Г. Методология риск-анализа и моделирования кибернетических систем, атакуемых вредоносным программным обеспечением [Электронный ресурс]: Учеб. пособие / А. Г. Остапенко, Д. Г. Плотников, С. В. Машин. - Электрон. текстовые, граф. дан. (112 Кб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2012. - 1 файл. - 30-00.

Эпидемии в телекоммуникационных сетях [Текст] / Остапенко Александр Григорьевич [и др.]; под ред. Д. А. Новикова. - Москва: Горячая линия - Телеком, 2014. - 282 с.: ил. - (Теория сетевых войн. № 1). - Библиогр.: с. 231-245 (244 назв.). - ISBN 978-5-9912-0682-2: 736-00

Дополнительная

1. Компьютерные преступления в сфере государственного и муниципального управления / В. Г. Кулаков, А. К. Соловьев, В. Г. Кобяшов; под. ред. А. Г. Остапенко. - Воронеж: ВИ МВД России, 2002. - 116 с. - ISBN 5-88591-002-4: 20.00.

2. Моделирование информационных операций и атак в сфере государственного и муниципального управления: Монография / под ред. В.И. Борисова. - Воронеж: ВИ МВД России, 2004. - 144 с. - 100-00.

3. Оптимальный синтез и анализ эффективности комплексов защиты информации: Монография / В. Г. Кулаков [и др.]. - Воронеж: ВГТУ, 2006. - 137 с. - 30-00

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

1. ООН [Официальный портал] - URL: http://www.un.org/ru.
2. Совет ЕВроiiы http://www.coe.int/ru.
3. СНГ [Официальный портал] - URL: http://www.e-cis.info.
4. Официальный интернет-портал правовой информации [Официальный портал] - URL: http://www.pravo.gov.ru.
5. Президент РФ [Официальный сайт] - URL: http://www.kremlin.ru.
6. Государственная Дума Федерального Собрания Российской Федерации [Официальный сайт] - URL: http://www.duma.gov.ru.
7. Совет Федерации Федерального Собрания Российской Федерации [Официальный сайт] - URL: http://www.council.gov.ru.
8. ПравительствоРФ [Официальный сайт] [Официальный портал] - URL: - URL:http://www.npaBin^bCTBO.p(biinH http://www.govemment.ru.
9. Конституционный Суд Российской Федерации [Официальный сайт] - URL:http://www.ksrf.ru.
10. Верховный Суд Российской Федерации [Официальный сайт] - URL:http:/, www.supcourt.ru.
11. «Юридическая Россия» - федеральный правовой портал [Официальный портал] - URL: http://law.edu.ru.
12. Российская государственная библиотека[Официальный сайт] - URL:http://www.rsl.ru.

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Специализированная лекционная аудитория, оснащенная оборудованием для лекционных демонстраций и проекционной аппаратурой

Дисплейный класс, оснащенный компьютерными программами для проведения практических занятий

10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «Компьютерные преступления в распределённых компьютерных системах» читаются лекции, проводятся практические занятия, выполняется курсовой проект.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Практические занятия направлены на приобретение практических навыков расчета

Неделя семестра	Тема и содержание практических занятий	Объем часов	Вид контроля
2	Анализ атаки, ориентированной на взлом программного обеспечения, путем обхода процедуры авторизации.	4	Лабораторная работа
4	Проведение анализа современного антивирусного программного обеспечения (Avira, Norton AntiVirus, Panda, Kaspersky, McAfee, NOD32, Avast, Dr.Web).	4	Практическая работа за компьютерами
5	Проведения сравнительной характеристики современных межсетевых экранов	4	Практическая работа за компьютерами
6	Проведение анализа работы сетевых сканеров. (Tcpdump, Sniffer Pro, NetXray, MS Network Monitor, Novell's LanAlyzer, Wireshark).	6	Практическая работа за компьютерами
7	Проведение анализа системы обнаружения вторжений Snort.	8	Практическая работа за компьютерами
8	Проведение сравнительного анализа уязвимостей в операционных системах.	8	Рефераты
9	Анализ уязвимостей PHP.	6	Рефераты
10	Анализ уязвимостей web-технологий	4	Рефераты
11	Проведение анализа подсистемы безопасности в семействе ОС Windows.	4	Практическая работа за
12	Проведение анализа подсистемы безопасности в ОС Unix.	6	Практическая работа за

13	Проведение сравнительного анализа уязвимостей в операционных системах.	4	Рефераты
14	Проведение сравнительного анализа Post и Get методов передачи данных в web.	4	Рефераты
15	Проведение анализа защищенности php-технологий.	4	Рефераты
16	Проведение анализа защищенности Java-приложений.	4	Рефераты
17	Проведение анализа работы троянских программ, взаимодействующих с USB-устройствами.	4	Рефераты

Занятия проводятся путем решения конкретных задач в аудитории.

Методика выполнения курсового проекта изложена в учебно-методическом пособии. Выполнять этапы курсового проекта должны своевременно и в установленные сроки.

Контроль усвоения материала дисциплины производится проверкой курсового проекта, защитой курсового проекта.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Практическое занятие	Конспектирование рекомендуемых источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы. Прослушивание аудио- и видеозаписей по заданной теме, выполнение расчетно-графических заданий, решение задач по алгоритму.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточной аттестации.
Подготовка к промежуточной аттестации	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные

	перед зачетом, зачетом, экзаменом три дня эффективнее всего использовать для повторения и систематизации материала.