МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ 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 распределенных компьютерных систем

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2017

Автор программы _____/Г.А. Остапенко/

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

Руководитель ОПОП _____/ А.Г. Остапенко /

Воронеж 2017

1.ЦЕЛИИЗАДАЧИДИСЦИПЛИНЫ

1.1.Целидисциплины

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.Задачиосвоениядисциплины

1.2.1. Привить навыки формирования требований по защите информации в различных КС.

1.2.2. Ознакомить с требованиями к защите автоматизированных информационных систем (ИС) от несанкционированного доступа (НСД) на территории Российской Федерации.

2.МЕСТОДИСЦИПЛИНЫВСТРУКТУРЕОПОП

Дисциплина«Компьютерныепреступлениявраспределённыхкомпьютерныхсистемах»относитсякдисциплинамвариативнойчастиблока Б1.

3.ПЕРЕЧЕНЬПЛАНИРУЕМЫХРЕЗУЛЬТАТОВОБУЧЕНИЯПОДИСЦИПЛИНЕ

Процессизучениядисциплины«Компьютерныепреступлениявраспределённыхкомпьютерныхсистемах»направленнаформированиеследующихкомпетенций:

ПСК-3.3-способностьюиспользоватьсовременныесредыитехнологии,разработкипрограммногообеспечениявраспределенныхкомпьютерныхсистемах сучётомтребованийинформационнойбезопасности

ПСК-3.4-способностьюорганизовыватьзащитуинформациивраспределенныхкомпьютерныхсистемах

Компетенция	Результатыобучения,характеризующие сформированностькомпетенции
ПСК-3.3	знатьосновные принципы построения защищенных РКС и построения систем обнаружения компьютерных атак, основные категории требований к программной и программно-аппаратной реализации средств защиты информации
	уметьобосновывать требования к программной и аппаратной реализации средств защиты
	владетьнавыками выявления и устранения уязвимостей компьютерной сети
ПСК-3.4	знатьособенности 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
	уметьанализировать защищенность систем, определять объекты защиты информации в КС и сетях
	владеть навыками проведения анализа рисков и администрирования безопасности распределенных компьютерных систем

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общаятрудоемкостьдисциплины«Компьютерныепреступлениявраспределённыхкомпьютерныхсистемах»составляет11з.е.

Распределениетрудоемкостидисциплиныповидамзанятий

очнаяформаобучения

Виды учебной работы	Всегочасов	Семестры		
		8	9	10
Аудиторные занятия (всего)	162	54	54	54
В том числе:				
Лекции	108	36	36	36
Лабораторные работы (ЛР)	54	18	18	18
Самостоятельная работа	198	54	72	72
Курсовой проект	+			+
Часы на контроль	36	-	-	36
Виды промежуточной аттестации - экзамен, зачет	+	+	+	+
Общая трудоемкость: академические часы зач.ед.	 396 11	 108 3	 126 3.5	 162 4.5

5.СОДЕРЖАНИЕДИСЦИПЛИНЫ(МОДУЛЯ)

5.1Содержаниеразделовдисциплиныираспределениетрудоемкостиповидамзанятий

очнаяформаобучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Лаб. зан.	СРС	Всего, час
1	Основы компьютерных преступлений	Понятие и разновидность компьютерных преступлений. Характеристика компьютерных преступлений	18	10	32	60
2	Расследование компьютерных преступлений	Обзор угроз политике безопасности компьютерных систем. Перечень моделей Раскрытие и расследование компьютерных преступлений. Законодательная основа борьбы с компьютерными преступлениями	18	10	32	60
3	Противодействие компьютерным преступлениям, осуществляемым с использованием вредоносного программного обеспечения	Детальный анализ вредоносного программного обеспечения. Классификация вирусов. Эвристический анализ. Анализ разрушающих воздействий программного	18	10	32	60

		обеспечения				
4	Противодействие компьютерным преступлениям, реализуемым в ходе проведения компьютерных сетевых атак	Компьютерные сетевые атаки.Удаленные компьютерные сетевые атаки: распределенные подходы организации. Системы обнаружения вторжения и межсетевого экранирования.	18	8	34	60
5	Противодействие компьютерным преступлениям путём реализации политики безопасности	Анализ разрушающих воздействий. Методы обнаружения и борьбы. Политики безопасности компьютерных систем. Организация сетевой политики безопасности	18	8	34	60
6	Предотвращение компьютерных преступлений в социальной и банковской сферах	Характеристика основных видов преступлений с использованием банковских пластиковых карт. Компьютерные преступления на социальные информационные сети. Предупреждение компьютерных преступлений.	18	8	34	60
		Итого	**108**	**54**	**198**	**360**

5.2Переченьлабораторныхработ

1. Лабораторная работа № 1. Анализ атаки, ориентированной на взлом программного обеспечения, путём обхода процедуры авторизации.

2. Лабораторная работа № 2.Проведение анализа современного антивирусного программного обеспечения (Avira, NortonAntiVirus, Panda, Kaspersky, McAfee, NOD32, Avast, Dr.Web).

3. Лабораторная работа № 3. Проведения сравнительной характеристики современных межсетевых экранов.

4. Лабораторная работа № 4.Проведение анализа работы сетевых сканеров. (Tcpdump, SnifferPro, NetXray, MS NetworkMonitor, Novell'sLanAlyzer, Wireshark).

5. Лабораторная работа № 5.Проведение анализа системы обнаружения вторжений Snort.

6. Лабораторная работа № 6.Проведение анализа подсистемы безопасности в семействе ОС Windows.

7. Лабораторная работа № 7.Проведение анализа подсистемы безопасности в ОС Unix.

6.ПРИМЕРНАЯТЕМАТИКАКУРСОВЫХПРОЕКТОВ(РАБОТ) ИКОНТРОЛЬНЫХРАБОТ

Всоответствиисучебнымпланомосвоениедисциплиныпредусматриваетвыполнениекурсовыхпроектовв10семестрахдляочнойформыобучения.

Примернаятематикакурсовогопроекта:«Расследование компьютерных преступлений в РКС, осуществляемых с использованием web-технологий»

Задачи,решаемыепривыполнениикурсовогопроекта:

• закрепить знание основных принципов построения защищённых РКС;

• закрепить знания особенностей защиты информации на узлах компьютерной сети, основные категории требований к программной и программно-аппаратной реализации средств защиты информации.

Курсовойпроектвключатвсебяграфическуючастьирасчетно-пояснительнуюзаписку.

7.ОЦЕНОЧНЫЕМАТЕРИАЛЫДЛЯПРОВЕДЕНИЯПРОМЕЖУТОЧНОЙАТТЕСТАЦИИОБУЧАЮЩИХСЯПОДИСЦИПЛИНЕ

7.1.Описаниепоказателейикритериевоцениванияикомпетенцийнаразличныхэтапахихформирования,описаниешкалоценивания

7.1.1Этаптекущегоконтроля

Результатытекущегоконтролязнанийимежсессионнойаттестацииоцениваютсяпоследующейсистеме:

«аттестован»;

«неаттестован».

Компе-тенция	Результатыобучения,характеризующие сформированностькомпетенции	Критерии оценивания	Аттестован	Неаттестован
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	Изучение лекционного материала, подготовка и отчёт по лабораторным и самостоятельным работам	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь обосновывать требования к программной и аппаратной реализации средств защиты	Изучение лекционного материала, подготовка и отчёт по лабораторным и самостоятельным работам	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть навыками выявления и устранения уязвимостей компьютерной сети	Изучение лекционного материала, подготовка и отчёт по лабораторным и самостоятельным работам	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	Изучение лекционного материала, подготовка и отчёт по лабораторным и самостоятельным работам	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	Изучение лекционного материала, подготовка и отчёт по лабораторным и	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих

	и сетях	самостоятельным работам		программах
	владеть навыками проведения анализа рисков и администрирования безопасности распределенных компьютерных систем	Изучение лекционного материала, подготовка и отчёт по лабораторным и самостоятельным работам	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2Этаппромежуточногоконтролязнаний

Результатыпромежуточногоконтролязнанийоцениваютсяв8,9,10семестредляочнойформыобученияподвух/четырехбалльнойсистеме:

«зачтено»

«незачтено»

Компе-тенция	Результатыобучения,характеризующие сформированностькомпетенции	Критерии оценивания	Зачтено	Незачтено
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	Изучение лекционного материала, зачёт	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь обосновывать требования к программной и аппаратной реализации средств защиты	Изучение лекционного материала, зачёт	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть навыками выявления и устранения уязвимостей компьютерной сети	Изучение лекционного материала, зачёт	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	Изучение лекционного материала, зачёт	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь анализировать защищенность систем, определять объекты	Изучение лекционного материала, зачёт	Выполнение работ в срок, предусмотренный в	Невыполнение работ в срок, предусмотренны

	защиты информации в КС и сетях		рабочих программах	й в рабочих программах
	владеть навыками проведения анализа рисков и администрирования безопасности распределенных компьютерных систем	Изучение лекционного материала, зачёт	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

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

Компе-тенция	**Результатыобучения,характеризующие сформированностькомпетенции**	**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	Изучение лекционного материала, экзамен	Ответ дан верно и в полном объеме	Ответ дан развёрнуто, продемонстрирован верный ход рассуждений, но не получен верный ответ по всем вопросам	Продемонстрирован верный ход рассужденийпобольшинствувопросов	Ответ на вопросы получен не был
	уметь обосновывать требования к программной и аппаратной реализации средств защиты	Изучение лекционного материала, экзамен	Ответ дан верно и в полном объеме	Ответ дан развёрнуто, продемонстрирован верный ход рассуждений, но не получен верный ответ по всем вопросам	Продемонстрирован верный ход рассужденийпобольшинствувопросов	Ответ на вопросы получен не был
	владеть навыками выявления и устранения уязвимостей компьютерной сети	Изучение лекционного материала, экзамен	Ответ дан верно и в полном объеме	Ответ дан развёрнуто, продемонстрирован верный ход рассуждений, но не получен верный ответ по всем вопросам	Продемонстрирован верный ход рассужденийпобольшинствувопросов	Ответ на вопросы получен не был
ПСК-3.4	знать особенности защиты информации на узлах компьютерной сети и концепцию защиты информации в государственных и коммерческих структурах, основные модели	Изучение лекционного материала, экзамен	Ответ дан верно и в полном объеме	Ответ дан развёрнуто, продемонстрирован верный ход рассуждений, но не получен верный ответ	Продемонстрирован верный ход рассужденийпобольшинствувопросов	Ответ на вопросы получен не был

	информационной безопасности и системные вопросы защиты программ и данных, основные категории требований к программной и программно-аппаратной реализации средств защиты информации			по всем вопросам		
	уметь анализировать защищенность систем, определять объекты защиты информации в КС и сетях	Изучение лекционного материала, экзамен	Ответ дан верно и в полном объеме	Ответ дан развёрнуто, продемонстрирован верный ход рассуждений, но не получен верный ответ по всем вопросам	Продемонстрирован верный ход рассужденийпобольшинствувопросов	Ответ на вопросы получен не был
	владеть навыками проведения анализа рисков и администрирования безопасности распределенных компьютерных систем	Изучение лекционного материала, экзамен	Ответ дан верно и в полном объеме	Ответ дан развёрнуто, продемонстрирован верный ход рассуждений, но не получен верный ответ по всем вопросам	Продемонстрирован верный ход рассужденийпобольшинствувопросов	Ответ на вопросы получен не был

7.2Примерныйпереченьоценочныхсредств(типовыеконтрольныезаданияилиныематериалы,необходимыедляоценкизнаний,умений,навыкови(или)опытадеятельности)

7.2.1Примерныйпереченьзаданийдляподготовкиктестированию

Не предусмотрено учебным планом

7.2.2Примерныйпереченьзаданийдлярешениястандартныхзадач

Не предусмотрено учебным планом

7.2.3Примерныйпереченьзаданийдлярешенияприкладныхзадач

Не предусмотрено учебным планом

7.2.4Примерныйпереченьвопросовдляподготовкикзачету

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. Атакитипа Main-in-the-Middle.

38. Атаки на уровне приложений. Противодействие.

39. Сетевая разведка. Злоупотребление доверием. Переадресация портов.

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.

7.2.5Примерныйпереченьзаданийдлярешенияприкладныхзадач

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 TakeGrant.

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. Атакитипа 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. Атакина IDS (FragmentationReassemblyTimeoutattacks, TTL

Basedattacks, OverlappingFragments).

80. Сигнатурные и поведенческие IDS.
81. Распределённые 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.Методикавыставленияоценкиприпроведенииипромежуточной аттестации

Зачёт проводится по билетам, каждый из которых содержит 2 вопроса. При достаточно полном правильном ответе не менее чем на 1вопрос, выполнении курсового проекта и сдаче его на положительную оценку студент получает оценку «Зачтено».

При отсутствии правильного ответа на вопросы, не выполнении курсового проекта или не сдаче его студент получает оценку «Не зачтено».

Экзаменпроводитсяпо билетам, каждый из которых содержит 2 вопроса.

1.Оценка«Неудовлетворительно»ставитсявслучае,еслистудентне ответил или ответил неверно на все вопросы билета.

2.Оценка«Удовлетворительно»ставитсявслучае,еслистудентпродемонстрировал верный ход рассуждений при ответе на вопросы, но правильные ответы получены не были.

3.Оценка«Хорошо»ставитсявслучае,еслистудент продемонстрировал верный ход рассуждений, но не в полной мере ответил на все вопросы.

4.Оценка«Отлично»ставится,еслистудентв полном объёме и верно ответил на все вопросы билета.

7.2.7Паспортоценочныхматериалов

№п/п	Контролируемыеразделы(темы)дисциплины	Кодконтролируемойкомпетенции	Наименованиеоценочногосредства
1	Основы компьютерных преступлений	ПСК-3.3, ПСК-3.4	Защита лабораторных работ, защита курсового проекта, зачёт, экзамен
2	Расследование компьютерных преступлений	ПСК-3.3, ПСК-3.4	Защита лабораторных работ, защита курсового проекта, зачёт, экзамен
3	Противодействие компьютерным преступлениям, осуществляемым с использованием вредоносного программного обеспечения	ПСК-3.3, ПСК-3.4	Защита лабораторных работ, защита курсового проекта, зачёт, экзамен
4	Противодействие компьютерным преступлениям, реализуемым в ходе проведения компьютерных сетевых атак	ПСК-3.3, ПСК-3.4	Защита лабораторных работ, защита курсового проекта, зачёт, экзамен
5	Противодействие компьютерным преступлениям путём реализации политики безопасности	ПСК-3.3, ПСК-3.4	Защита лабораторных работ, защита курсового проекта, зачёт, экзамен
6	Предотвращение компьютерных преступлений в социальной и банковской сферах	ПСК-3.3, ПСК-3.4	Защита лабораторных работ, защита курсового проекта, зачёт, экзамен

7.3.Методическиематериалы,определяющиепроцедурыоцениванияознаний,умений,навыкови(или)опытадеятельности

Тестированиеосуществляется,либоприпомощикомпьютернойсистемытестирования,либосиспользованиемвыданныхтест-заданийнабумажномносителе.Времятестирования30мин.Затемосуществляетсяпроверкатестаэкзаменатором,ивыставляетсяоценкасогласнометодикивыставленияоценкиприпроведенииромежуточнойаттестации.

Решениестандартныхзадачосуществляется,либоприпомощикомпьютернойсистемытестирования,либосиспользованиемвыданныхзадачнабумажномносителе.Времярешениязадач30мин.Затемосуществляетсяпроверкарешениязадачэкзаменатором,ивыставляетсяоценка,согласнометодикивыставленияоценкиприпроведенииромежуточнойаттестации.

Решениеприкладныхзадачосуществляется,либоприпомощикомпьютернойсистемытестирования,либосиспользованиемвыданныхзадачнабумажномносителе.Времярешениязадач30мин.Затемосуществляетсяпроверкарешениязадачэкзаменатором,ивыставляетсяоценка,согласнометодикивыставленияоценкиприпроведенииромежуточнойаттестации.

Защитакурсовойработы,курсовогопроектаилиотчетаповсемвидампрактикосуществляетсясогласнотребованиям,предъявляемымкработе,описаннымвметодическихматериалах.Примерноевремязащитынаодногостудентасоставляет20мин.

8УЧЕБНОМЕТОДИЧЕСКОЕИИНФОРМАЦИОННОЕ

ОБЕСПЕЧЕНИЕДИСЦИПЛИНЫ)

8.1Переченьучебнойлитературы,необходимойдляосвоениядисциплины

Основная литература:

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.
3. 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.

681.3
Э 71
Эпидемии в телекоммуникационных сетях [Текст] / под ред. Д. А. Новикова. - Москва : Горячая линия - Телеком, 2017. - 282 с. : ил. - (Теория сетевых войн. № 1). - Библиогр.: с. 231-245 (244 назв.). - ISBN 978-5-9912-0682-2 : 300-00.

Дополнительная литература:

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

8.2Переченьинформационныхтехнологий,используемыхприосуществленииобразовательногопроцессаподисциплине,включаяпереченьлицензионногопрограммногообеспечения,ресурсовинформационно-телекоммуникационнойсети«Интернет»,современныхпрофессиональныхбазданныхиинформационныхсправочныхсистем:

1. Сайт кафедры СИБ.
2. Сайт Банка данных угроз безопасности информации ФСТЭК России.
3. Международная система «Интернет».
4. Анализатор сетевого трафика Wireshark.

5. Система обнаружения вторжений Snort.

6. Операционная система Kali Linux, содержащая средства демонстрации компьютерных атак.

9МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯБАЗА,НЕОБХОДИМАЯДЛЯОСУЩЕСТВЛЕНИЯОБРАЗОВАТЕЛЬНОГОПРОЦЕССА

1. Комплект действующих нормативных документов в области компьютерных преступлений и обеспечения безопасности информационных систем.

2. Компьютерный класс и компьютерные программы для демонстрации компьютерных сетевых атак и мер защиты от них.

3. Проектор и ноутбук.

10.МЕТОДИЧЕСКИЕУКАЗАНИЯДЛЯОБУЧАЮЩИХСЯПООСВОЕНИЮДИСЦИПЛИНЫ(МОДУЛЯ)

Подисциплине«Компьютерныепреступлениявраспределённыхкомпьютерныхсистемах»читаютсялекции,проводятсялабораторныеработы,выполняетсякурсовойпроект.

Основойизучениядисциплиныявляютсялекции,накоторыхизлагаютсяналиболеесущественныеитрудныевопросы,атакжевопросы,ненашедшиеотражениявучебнойлитературе.

Лабораторныеработывыполняютсяналабораторномоборудованиивсоответствиисметодиками,приведеннымивуказанияхквыполнениюработ.

Методикавыполнениякурсовогопроектаизложенавучебно-методическомпособии.Выполнятьэтапыкурсовогопроектадолжнысвоевременноивустановленныесроки.

Контрольусвоенияматериаладисциплиныпроизводитсяпроверкойкурсовогопроекта,защитойкурсовогопроекта.

Видучебныхзанятий	Деятельностьстудента
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.
Лабораторнаяработа	Лабораторные работы позволяют научиться применять теоретические знания, полученные на лекции при решении конкретных задач. Чтобы наиболее рационально и полно использовать все возможности лабораторных для подготовки к ним необходимо: следует разобрать лекцию по соответствующей теме, ознакомится с соответствующим разделом учебника, проработать дополнительную литературу и источники, решить

	задачи и выполнить другие письменные задания.
Самостоятельнаяработа	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 промежуточнойаттестации.
Подготовка к промежуточнойаттестации	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.