МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета _____ Гусев П.Ю.

«31» августа 2021 г.

РАБОЧАЯ ПРОГРАММА

дисциплины

«Компьютерные преступления в информационных системах и сетях»

Специальность 10.05.03 Информационная безопасность автоматизированных систем

Специализация специализация N 7 "Анализ безопасности информационных систем"

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2021

Автор программы _____ /Сердечный А.Л./

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

Руководитель ОПОП _____ /Остапенко А.Г./

Воронеж 2021

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели 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

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. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Компьютерные преступления в информационных системах и сетях» относится к дисциплинам части, формируемой участниками образовательных отношений (дисциплина по выбору) блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Компьютерные преступления в информационных системах и сетях» направлен на формирование следующих компетенций:

ПК-7.3 - Способен участвовать в проведении криминалистического анализа автоматизированных систем

ПК-7.2 - Способен разрабатывать проектные решения по защите информации в автоматизированных системах

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ПК-7.3	знать
	уметь
	владеть
ПК-7.2	знать
	уметь
	владеть

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Компьютерные преступления в информационных системах и сетях» составляет 16 з.е.

Распределение трудоемкости дисциплины по видам занятий **очная форма обучения**

Виды учебной работы	Всего часов	Семестры	
		9	10
Аудиторные занятия (всего)	216	108	108
В том числе:			
Лекции	72	36	36
Лабораторные работы (ЛР)	144	72	72
Самостоятельная работа	288	144	144
Часы на контроль	72	36	36
Виды промежуточной аттестации - экзамен	+	+	+
Общая трудоемкость: академические часы зач.ед.	576 16	288 8	288 8

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	Лаб. зан.	СРС	Всего, час
1	Основы компьютерных преступлений	Понятие и разновидность компьютерных преступлений. Характеристика компьютерных преступлений	12	24	48	84
2	Расследование компьютерных преступлений	Обзор угроз политике безопасности компьютерных систем. Перечень моделей Раскрытие и расследование компьютерных преступлений. Законодательная основа борьбы с компьютерными преступлениями	12	24	48	84
3	Противодействие с компьютерным преступлениям, осуществляемым использованием вредоносного программного обеспечения	Детальный анализ вредоносного программного обеспечения. Классификация вирусов. Эвристический анализ. Анализ разрушающих воздействий программного обеспечения	12	24	48	84

4	Противодействие компьютерным преступлениям, реализуемым ходе проведения компьютерных сете атак	Компьютерные сетевые атаки. Удаленные компьютерные сетевые атаки: распределенные подходы организации. Системы обнаружения вторжения и межсетевого экранирования.	12	24	48	84
5	Противодействие компьютерным преступлениям путём реализации политики безопасности	Анализ разрушающих воздействий. Методы обнаружения и борьбы. Политики безопасности компьютерных систем. Организация сетевой политики безопасности	12	24	48	84
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.	12	24	48	84
		Итого	**72**	**144**	**288**	**504**

5.2 Перечень лабораторных работ

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, Norton AntiVirus, 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, Sniffer Pro, NetXray, MS Network Monitor, Novell's LanAlyzer, 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. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины предусматривает выполнение курсовых проектов в 10 семестрах для очной формы обучения.

Примерная тематика курсового проекта: «Расследование компьютерных преступлений в РКС, осуществляемых с использованием web-технологий»

Задачи, решаемые при выполнении курсового проекта:

• 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.

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».

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ПК-7.3	знать (переносится из раздела 3 рабочей программы)	укажите критерий	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь (переносится из раздела 3 рабочей программы)	укажите критерий	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть (переносится из раздела 3 рабочей программы)	укажите критерий	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-7.2	знать (переносится из раздела 3 рабочей программы)	укажите критерий	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь (переносится из раздела 3 рабочей программы)	укажите критерий	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть (переносится из раздела 3 рабочей программы)	укажите критерий	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 9, 10 семестре для очной формы обучения по четырехбалльной системе:

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Отлично	Хорошо	Удовл.	Неудовл.
ПК-7.3	знать (переносится из раздела 3 рабочей программы)	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь (переносится из раздела 3 рабочей программы)	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 (переносится из раздела 3 рабочей программы)	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
ПК-7.2	знать (переносится из раздела 3 рабочей программы)	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь (переносится из	Решение стандартных	Задачи решены в	Продемонстрирован	Продемонстрирован верный	Задачи не решены
	раздела 3 рабочей программы)	практических задач	полном объеме и получены верные ответы	верный ход решения всех, но не получен верный ответ во всех задачах	ход решения в большинстве задач	
	владеть (переносится из раздела 3 рабочей программы)	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

Не предусмотрено учебным планом

7.2.2 Примерный перечень заданий для решения стандартных задач

Не предусмотрено учебным планом

7.2.3 Примерный перечень заданий для решения прикладных задач

Не предусмотрено учебным планом

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 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.

7.2.5 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. 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. Методика выставления оценки при проведении промежуточной аттестации

Зачёт проводится по билетам, каждый из которых содержит 2 вопроса. При достаточно полном правильном ответе не менее чем на 1 вопрос, 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».

Экзамен проводится по билетам, каждый из которых содержит 2 вопроса.

1. Оценка «Неудовлетворительно» ставится в случае, если студент не ответил или ответил неверно на все вопросы билета.

2. Оценка «Удовлетворительно» ставится в случае, если студент продемонстрировал верный ход рассуждений при ответе на вопросы, но правильные ответы получены не были.

3. Оценка «Хорошо» ставится в случае, если студент продемонстрировал верный ход рассуждений, но не в полной мере ответил на все вопросы.

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

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	(наименование темы из раздела 5.1)	ПК-7.3, ПК-7.2	Экзамен
2	(наименование темы из раздела 5.1)	ПК-7.3, ПК-7.2	Экзамен

3	(наименование темы из раздела 5.1)	ПК-7.3, ПК-7.2	Экзамен
4	(наименование темы из раздела 5.1)	ПК-7.3, ПК-7.2	Экзамен
5	(наименование темы из раздела 5.1)	ПК-7.3, ПК-7.2	Экзамен
6	(наименование темы из раздела 5.1)	ПК-7.3, ПК-7.2	Экзамен

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.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

Основная литература:

1. Эпидемии в телекоммуникационных сетях [Текст] / под ред. Д. А. Новикова. - Москва : Горячая линия - Телеком, 2018. - 282 с. : ил. - (Теория сетевых войн. № 1). - Библиогр.: с. 231-245 (244 назв.). - ISBN 978-5-9912-0682-2 : 736-00.

2. Атакуемые взвешенные сети [Текст] / под ред. Д. А. Новикова. - Москва : Горячая линия - Телеком, 2018. – 247 с. : ил. - (Теория сетевых войн. № 2). - Библиогр.: с. 201-213 (214 назв.). - ISBN 978-5-9912-0684-6 : 708-00.

3. Социальные сети и деструктивный контент [Текст] / под ред. Д. А. Новикова. - Москва : Горячая линия - Телеком, 2018. - 274 с. : ил. - (Теория сетевых войн. № 3). - Библиогр.: с. 224-239 (278 назв.). - ISBN 978-5-9912-0686-0 : 719-00.

4. 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.

5. 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.

Дополнительная литература:

1. Обнаружение сетевых вторжений [Электронный ресурс] : Учеб. пособие. - Электрон. текстовые, граф. дан. (423 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2013. - 1 файл. - 30-00.

2. Модели обнаружения сетевых вторжений [Электронный ресурс] : Учеб. пособие. - Электрон. текстовые, граф. дан. (652 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2013. – 1 файл. - 30-00.

3. Методические указания к курсовому проектированию по дисциплине «Компьютерные преступления в распределенных компьютерных системах» для студентов специальности 090301 «Компьютерная безопасность» очной формы обучения [Электронный ресурс] / Каф. систем информационной безопасности; Сост.: Г. А. Остапенко, А. Е. Дешина. - Электрон. текстовые, граф. дан. (820 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2015. – 1 файл. - 00-00.

4. Методические указания к самостоятельным работам по дисциплине «Компьютерные преступления в распределенных компьютерных системах» для студентов специальности 090301 «Компьютерная безопасность» очной формы обучения [Электронный ресурс] / Каф. систем информационной безопасности; Сост.: Г. А. Остапенко, А. Е. Дешина. -

Электрон. текстовые, граф. дан. (427 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2015. – 1 файл. - 00-00.

5. Остапенко, Г.А. Логико-лингвистические модели атак на компьютерные системы [Электронный ресурс] : Учеб. пособие / под ред. А. Г. Остапенко. - Электрон. текстовые, граф. дан. (8452435 байт). - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2008. – 1 файл. - 30-00.

6. 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.

7. Остапенко, Г.А. Компьютерные преступления [Электронный ресурс] : Учеб. пособие. - Электрон. текстовые, граф. дан. (1,37 Мб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет",
2013. - 1 файл. - 30-00.

8. Дуров В.П. Программно-аппаратная защита информации
[Электронный ресурс] : учеб. пособие. - Электрон. дан. (1 файл :6681088 байт). - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2006. – 1 файл. - 30-00.

9. 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.

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

11. Остапенко, Г.А. Нейронные модели обнаружения вторжений и атак на компьютерные сети [Электронный ресурс] : учеб. пособие. - Электрон. дан. (1 файл : 2402Кб). - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2007. - 1 файл. - 30-00.

12. Щербаков, В.Б. Обнаружение вторжений на основе анализа фрагментов унитарного кода [Электронный ресурс] : учеб. пособие. -
Электрон. дан. (1 файл : 1454 Кб). - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2007. - 1 файл. - 30-00.

13. Пархоменко, А.П. Основные проблемы и особенности защиты информации в банковских системах: модели нарушителей [Электронный ресурс] / под ред. Г. С. Остапенко. - Электрон. текстовые, граф. дан. (

1245435 байт). - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2008. - 1 файл. - 30-00

14. Компьютерные преступления [Электронный ресурс] : Методические указания к выполнению практических занятий по учебной дисциплине "Компьютерные преступления в распределительных компьютерных системах" для студентов специальности 090301 "Компьютерная безопасность" очной формы обучения / Каф. систем информационной безопасности; Сост.: Г.
А. Остапенко, К. В. Симонов. - Электрон. текстовые, граф. дан. (3478 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2012. - 1 файл. - 00-00.

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. Сайт кафедры СИБ.
2. Сайт Банка данных угроз безопасности информации ФСТЭК России.
3. Информационные карты «Научные публикации по дисциплине "Компьютерные преступления"», «Публикации информационного ресурса Хабр, имеющие отношение к дисциплине "Компьютерные преступления"», «Средства тестирования на проникновение».
4. Международная система «Интернет».
5. Операционная система Kali Linux, содержащая средства демонстрации компьютерных атак, а также средства контроля защищённости информационных систем методом тестирования на проникновение.
6. Банк данных угроз безопасности информации. Электрон. дан. - Режим доступа: http://www.bdu.fstec.ru
7. Стандарт Common Vulnerabilities and Exposures. Электрон. дан. - Режим доступа: http://cve.mitre.org
8. База данных с информационными бюллетенями (Secunia Advisories), содержащими сведения об обнаруженных угрозах и уязвимостях ПО Secunia Advisory and Vulnerability Database Электрон. дан. - Режим доступа: https://secuniaresearch.flexerasoftware.com/community/advisories
9. База уязвимостей VND (Vulnerability Notes Database Электрон. дан. - Режим доступа: https://www.kb.cert.org/vuls
10. База сценариев эксплуатации уязвимостей Exploit Database Электрон. дан. - Режим доступа: https://www.exploit-db.com

11. Агрегатор информации об уязвимостях CVEDetails. Электрон. дан. - Режим доступа: https://www.cvedetails.com

12. Information Security Информационная безопасность. Электрон. дан. - Режим доступа: http://www.itsec.ru

13. Securitylab.ru by Positive Technologies. Электрон. дан. - Режим доступа: https://www.securitylab.ru/

14. Anti-Malware.ru. Электрон. дан. - Режим доступа: https://www.anti-malware.ru/news

15. Iso27000.ru Искусство управления информационной безопасностью. Электрон. дан. - Режим доступа: http://www.iso27000.ru/

16. SecurityPolicy.ru Документы по информационной безопасности. Электрон. дан. - Режим доступа: http://securitypolicy.ru/

17. SearchInform – Информационная безопасность. Электрон. дан. - Режим доступа: https://searchinform.ru/informatsionnaya-bezopasnost/

18. Информационная безопасность предприятия. Электрон. дан. - Режим доступа: Ekrost.ru

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

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. Проектор и ноутбук.

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

По дисциплине «Компьютерные преступления в информационных системах и сетях» читаются лекции, проводятся лабораторные работы.

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

Лабораторные работы выполняются на лабораторном оборудовании в соответствии с методиками, приведенными в указаниях к выполнению работ.

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.
Лабораторная работа	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.
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 экзаменом, экзаменом три дня эффективнее всего использовать для повторения и систематизации материала.